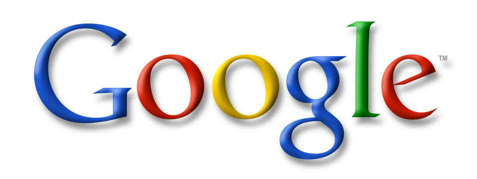
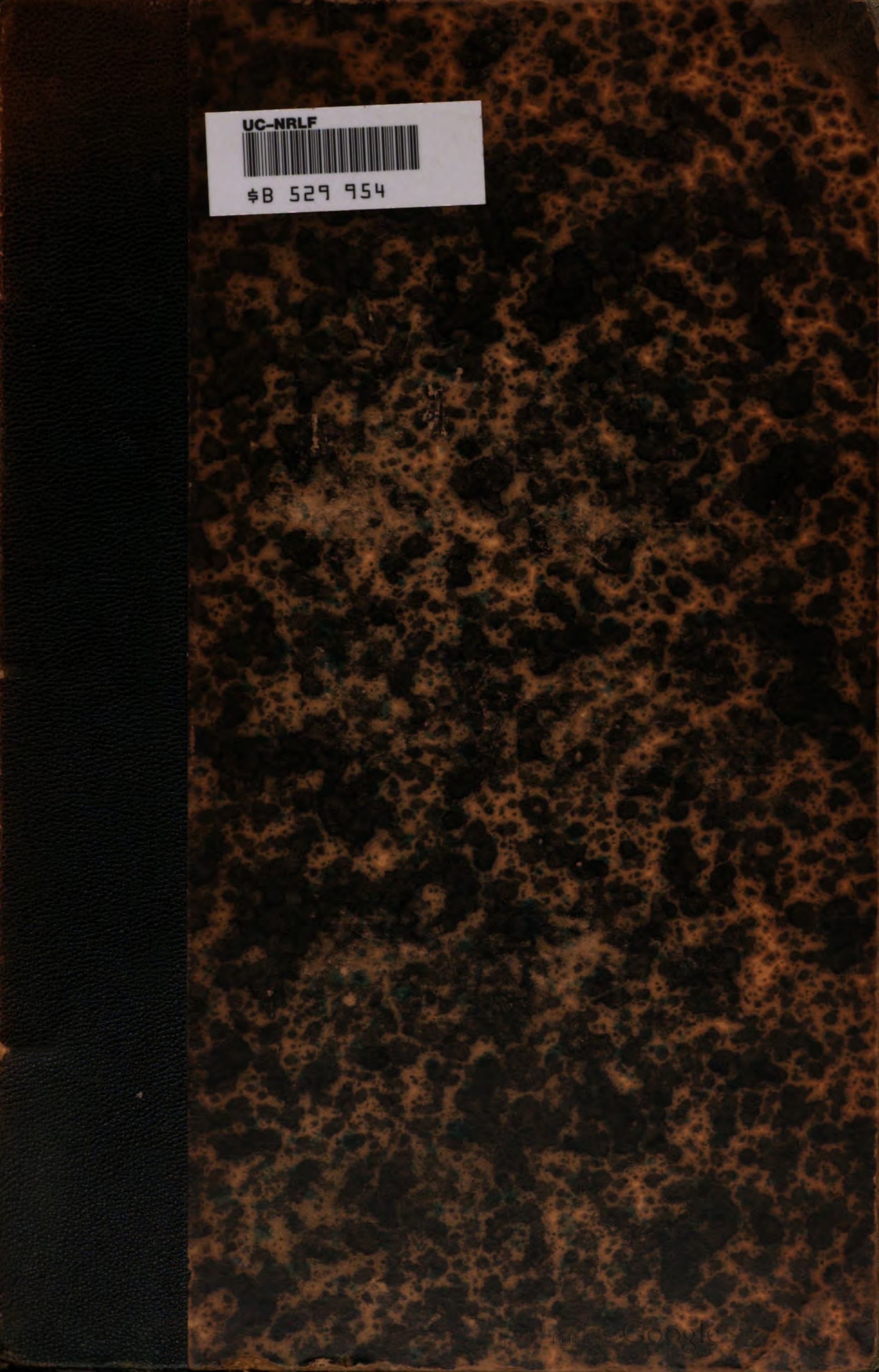
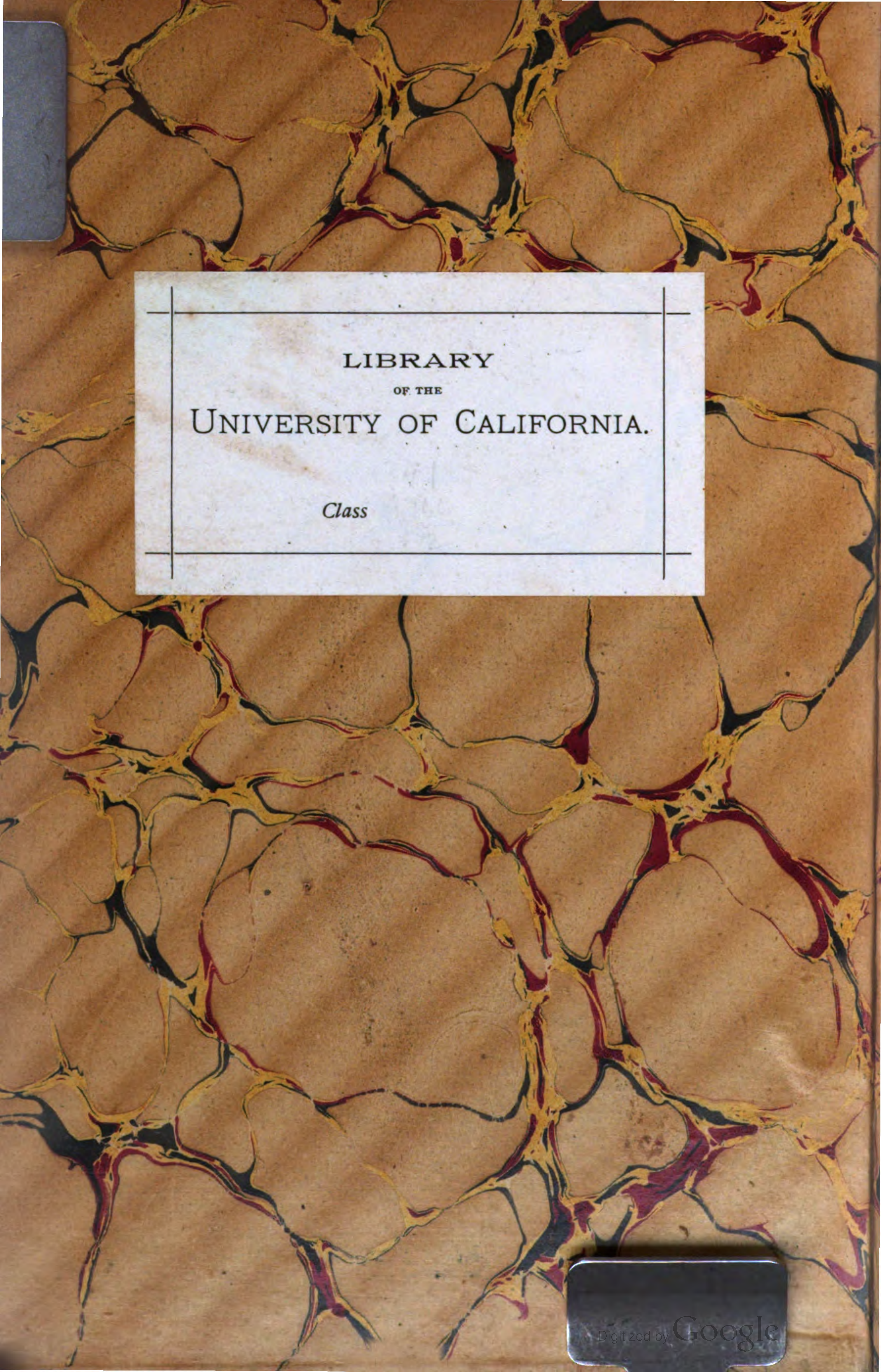
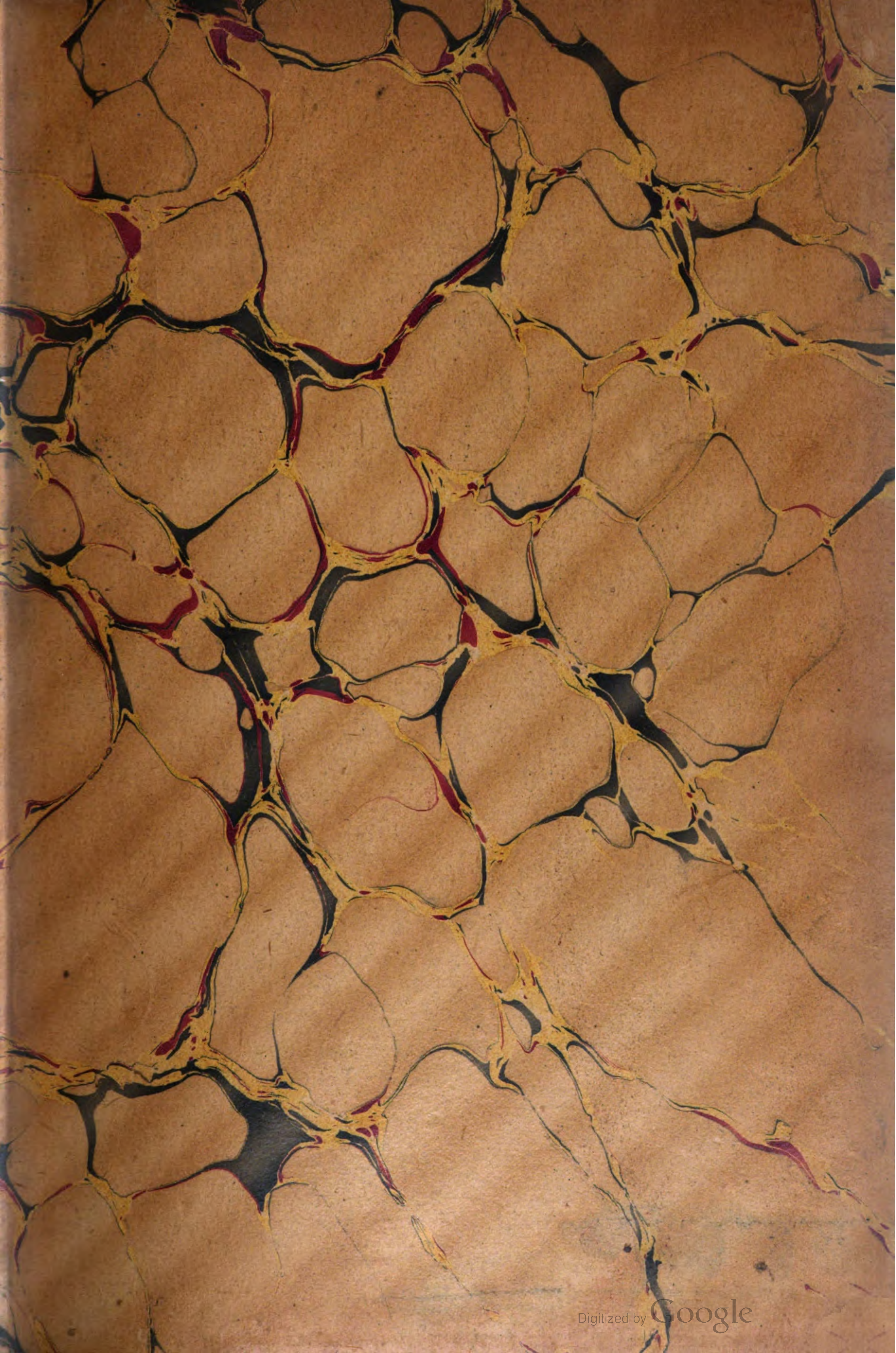





LIBRARY
OF THE
UNIVERSITY OF CALIFORNIA.
Class
Digitized by Google



ESSAIS DE PSYCHOLOGIE ET DE MÉTAPHYSIQUE POSITIVES.

ARITHMÉTIQUE GRAPHIQUE.

INTRODUCTION

A

L'ÉTUDE DES FONCTIONS ARITHMÉTIQUES,

PAR GABRIEL ARNOUX,

ANCIEN OFFICIER DE MARINE.

Gardons-nous de croire qu'une science est faite, quand on l'a réduite à des formules analytiques. Rien ne nous dispense d'étudier les choses en elles-mêmes, et de nous bien rendre compte des idées qui font l'objet de nos spéculations. (POINSOT, *Théorie nouvelle de la rotation des corps*.)



PARIS,

GAUTHIER-VILLARS, IMPRIMEUR-LIBRAIRE

DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE,

Quai des Grands-Augustins, 55.

1906

ARITHMÉTIQUE GRAPHIQUE.

INTRODUCTION

A

L'ÉTUDE DES FONCTIONS ARITHMÉTIQUES.

PARIS. — IMPRIMERIE GAUTHIER-VILLARS,
36964 Quai des Grands-Augustins, 55.

ESSAIS DE PSYCHOLOGIE ET DE MÉTAPHYSIQUE POSITIVES.

ARITHMÉTIQUE GRAPHIQUE.

INTRODUCTION

A

L'ÉTUDE DES FONCTIONS ARITHMÉTIQUES,

PAR GABRIEL ARNOUX,

ANCIEN OFFICIER DE MARINE.

Gardons-nous de croire qu'une science est faite, quand on l'a réduite à des formules analytiques. Rien ne nous dispense d'étudier les choses en elles-mêmes, et de nous bien rendre compte des idées qui font l'objet de nos spéculations. (POINSOT, *Théorie nouvelle de la rotation des corps*.)



PARIS,

GAUTHIER-VILLARS, IMPRIMEUR-LIBRAIRE

DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE,

Quai des Grands-Augustins, 55.

1906

PRÉFACE.

Ce Livre n'est point un Traité didactique sur les fonctions arithmétiques, mais plutôt une simple causerie sur ce sujet si intéressant et si peu connu.

Aujourd'hui, le champ des Mathématiques est si vaste que les hommes même de la plus haute valeur sont obligés de se cantonner dans certaines provinces, si je puis ainsi m'exprimer, n'ayant qu'une idée très succincte de ce qui ne concerne pas leur spécialité.

J'ai espéré leur être agréable en résumant, dans un petit et modeste Volume, les principes les plus essentiels de ce chapitre de la Science des nombres.

Visuel à un haut degré, il m'a semblé que la méthode graphique pourrait, dans beaucoup de parties, prêter à la Science un puissant secours, tant au point de vue théorique qu'au point de vue pratique.

J'ai appuyé sur les considérations concrètes, persuadé qu'elles sont le moyen le plus sûr d'initier aux considérations abstraites, et de les graver dans la mémoire d'une façon indélébile.

Il porte comme nom d'auteur celui de *Gabriel Arnoux;* à ce point de vue il est inexact, il devrait porter également celui de *C.-A. Laisant.* Je m'explique : la division du travail est une nécessité aujourd'hui universellement reconnue; pour que la Science progresse, il faut la collaboration de deux genres de travailleurs, les inventeurs et ceux qui se chargent de mettre les inventions à la portée du public.

Chacun d'eux, dans la spécialité qui le concerne, doit procéder

d'une façon différente, posséder des dispositions naturelles particulières, les cultiver, les développer de manière à acquérir une sorte de supériorité pour le genre de travail auquel il s'est voué.

L'inventeur n'a de chance de réussir qu'en s'adonnant exclusivement à des sujets qui l'intéressent, et ne les attaquant qu'au moment précis où il éprouve pour certaines parties une sorte d'appétence.

Il est le serviteur de son organisme, qui règne en souverain absolu. Si, dans le travail d'invention, le *moi* veut intervenir, il le fait en général d'une façon si maladroite, qu'il entrave l'œuvre de son associé au lieu de lui venir en aide. Tout ce qu'il peut faire, c'est de le mettre à même de travailler en lui fournissant les moyens d'acquérir les matériaux nécessaires. Cette première opération exécutée, il doit assister en spectateur à l'opération, qui est une sorte de cristallisation. Quand elle est accomplie, l'organisme, qui a fait un travail de synthèse des éléments qui lui ont été fournis, lui donne le résultat sous une forme intuitive; il n'a plus qu'à l'enregistrer.

L'organisme perçoit une foule de choses que le moi ne distingue pas; ainsi, vous lisez un livre, vous croyez n'y avoir rien compris, ne vous en être rien assimilé; erreur.

La partie profonde du sujet traité a été saisie dans ce qui concerne le territoire de vos hémisphères qui, par le fait de l'héritage ancestral ou de l'éducation, a acquis chez vous une prédominance spéciale.

Si, par un travail consciencieux d'analyse ultérieure, vous revenez sur ce sujet, vous vous apercevez que bien des idées que vous croyez avoir créées de toutes pièces vous viennent de votre prédécesseur, que vous n'avez fait que les lui emprunter, en les adaptant à votre spécialité cérébrale.

Dans cette œuvre d'invention, quelle est la part qui revient à chacun? il serait bien difficile de le dire: bien souvent, c'est un inconnu dont tout le monde ignore le nom, qui a passé inaperçu, qui est le grand précurseur.

En général, on pourrait même dire que les hommes à grande

renommée, que l'on proclame comme les maîtres de la Science, sont inconsciemment de grands pillards prenant leur bien où ils le trouvent.

Est-ce à dire que ce sont de simples voleurs? nullement. Ils ont pris l'œuvre de leurs prédécesseurs inconnus, se la sont assimilée, l'ont travaillée conformément aux parties prédominantes de leur organisme, ce que Taine appelait la *qualité maîtresse*, et ont obtenu des produits supérieurs, qu'ils offrent au public comme leur appartenant exclusivement.

J'ai pu personnellement me convaincre du fait.

Quant au hasard dans les inventions, son rôle est bien simple; quand vous avez tourné, retourné, ressassé une question, votre cerveau, par cela même, a été modifié; or, principe fondamental : *on ne voit jamais que ce qui se passe dans son cerveau.* Dire, par exemple, qu'on voit une étoile est une manière de parler; on ne voit en réalité que l'impression produite sur le mécanisme nerveux par les rayons émanés de l'étoile depuis un temps plus ou moins long, de sorte que, dans la direction où vous regardez, il est certain que l'étoile ne se trouve pas.

A mesure que votre cerveau travaille, ses parties matérielles se modifient; elles sont susceptibles d'être différemment impressionnées, vous voyez par suite ce que vous étiez dans l'impossibilité de voir auparavant; *or, qu'est-ce qu'inventer? c'est voir.*

Le milieu ambiant contient une foule de choses dont les parties évoluent et produisent des combinaisons diverses; la coïncidence fortuite qu'on nomme *hasard* met devant vous une de ces combinaisons; vous ne la distinguez que si votre organisation cérébrale a été modifiée d'une manière appropriée. Hier, vous ne voyiez pas certains phénomènes; aujourd'hui, vous les distinguez nettement. Demain, d'autres faits, qui aujourd'hui passent inaperçus devant vous, vous frapperont. Voilà la part du hasard. Il ne favorise que les habiles et les persévérants.

Le moi de l'inventeur n'a conscience, tout d'abord, que des parties les plus spéciales de son sujet, celles-là seules le frappent;

s'il est doué de ténacité et de persévérance, conditions indispensables pour la réussite, il poursuit son œuvre; à mesure que les faits singuliers deviennent familiers, ils cessent de l'impressionner; des faits de plus en plus généraux lui apparaissent et, ce mécanisme continuant à fonctionner, il en arrive à percevoir les considérations fondamentales. Si bien qu'il y a une distance colossale entre un individu, quand il commence un travail, et ce même individu, quand il l'achève : le premier est un apprenti; le second, un maître.

C'est alors qu'il doit appeler à son aide le travailleur qui s'est adonné à l'exposition.

Il est bien rare que les deux genres de qualités nécessaires à l'invention et à l'exposition soient réunis dans le même individu, et tel qui inventera assez facilement est incapable de montrer ses trouvailles au public.

Mais rien ne s'oppose à la collaboration.

Les qualités de celui qui expose sont toutes différentes : il doit posséder une grande facilité d'assimilation, percevoir les ensembles, éviter les répétitions, distinguer l'ordre d'importance et celui de succession des parties, de manière à faire passer le lecteur, des idées qu'il possède au moment où il ouvre le livre, à celles qu'on désire lui faire acquérir, et cela avec un minimum de travail mental.

Les lecteurs ont été de tout temps fort exigeants; ils le sont davantage encore aujourd'hui.

Pour voyager dans un territoire scientifique, si ardu qu'il soit, ils veulent des wagons bien confortables, qui les conduisent mollement du point de départ au point d'arrivée. Nous sommes bien loin de l'époque où Euclide disait à Ptolémée qu'il n'est point de routes royales pour la Science.

L'art de l'exposition a fait aujourd'hui de tels progrès, que le public n'accepte plus l'infériorité dans ce genre, et jette dédaigneusement de côté toute œuvre, fût-elle d'une valeur incontestable, qui lui présente une trop grande difficulté de lecture.

Quand je m'occupais d'Algèbre graphique, mon libraire me mit

entre les mains une étude sur les équipollences signée *Laisant*. Le talent d'exposition me frappa, et je n'eus de repos que quand j'eus obtenu la collaboration de ce maître en l'art d'exposer.

C'est lui qui a rédigé toute la partie mathématique de mon Étude sur les espaces arithmétiques hypermagiques; c'est lui encore qui vient de rédiger le présent Volume. Un des principes fondamentaux dans la recherche de la vérité est l'honnêteté absolue de la pensée et de la conduite en tout et partout.

La vérité n'accorde ses faveurs qu'à ceux qui l'adorent; on ne la trompe pas, et elle est impitoyable pour ceux qui ne l'aiment pas exclusivement. Franklin disait :

« Si les coquins connaissaient tous les avantages de l'honnêteté, ils deviendraient honnêtes par coquinerie. »

Et puis, à quoi bon mentir? Pour faire croire que votre organisme possède une supériorité personnelle que la nature lui a refusée, et mériter ainsi, non l'admiration, mais le mépris des hommes compétents, seuls juges en une pareille matière.

La collaboration n'est pas moins utile dans l'invention, surtout quand les collaborateurs ont des hémisphères dont les formules cérébrales ne sont pas les mêmes.

Ainsi, prenez un visuel et un symboliste, leurs formules hémisphériques sont notablement différentes; ce ne sont pas les mêmes territoires qui prédominent; dans une chasse en commun, chacun d'eux perçoit des considérations différentes et les apporte au stock des acquisitions successives. Si l'un a avancé la question sur un sujet à son point de vue, l'autre s'en saisit immédiatement et la fait progresser au sien et, bien souvent, de cet attelage, il résulte des solutions qui auraient bravé des efforts isolés.

L'un des collaborateurs complète l'autre, et de leur union résulte une sorte d'individu doué de facultés multiples.

Dans cette recherche en commun, quelle est la part de découverte qui revient à l'un et à l'autre? il serait bien difficile de le dire; il arrive même bien souvent qu'une pensée, une idée, est pour ainsi dire dans l'air, et que les deux associés la saisissent

simultanément; il serait oiseux de soulever une question de priorité qui, au point de vue de la Science, n'a aucune utilité. En principe, chacun perçoit ce qui a rapport à sa faculté maîtresse, et l'essentiel pour le public est que la chasse soit fructueuse.

Je me suis bien souvent demandé s'il n'y aurait pas lieu de créer des *monastères scientifiques,* dans lesquels les savants entreraient et sortiraient librement, sans vœux d'aucune espèce, lieux de refuge et d'isolement où des individus différemment doués, s'intéressant à une même question, pourraient, à l'abri des agitations du milieu ambiant, déchargés des soins de la vie matérielle, ayant à leur disposition une bibliothèque spéciale contenant tout ce qui est actuellement connu, faire progresser la Science.

Ces monastères devraient naturellement être absolument internationaux, et ceux qui y entreraient déposeraient en entrant au vestiaire leurs habits politiques et leur nationalité, tristes sujets de haine, qui ruinent l'humanité au profit de quelques intrigants sans valeur réelle, qui exploitent cette pomme de discorde.

Dans les guerres qui pourraient s'élever encore, avant que l'humanité tout entière ne soit réunie en une seule nation, ces monastères pourraient d'un commun accord être respectés par les belligérants, comme neutres, et chaque nation, chaque individu s'intéressant à la Science pourrait faire des dons et des legs, pour créer un capital qui, exempt de toute imposition, pourvoirait aux dépenses inévitables d'une pareille institution. Il me semble inutile de dire que les idées de religion seraient rigoureusement exclues de ce temple de la Science.

Cet Ouvrage portant le titre : *Essais de psychologie et de métaphysique positives,* le lecteur m'excusera sans doute de traiter dans ma préface une question de psychologie.

Dès mon enfance, j'ai reconnu dans mon organisme une certaine facilité d'invention et, quand je commençai à étudier les Mathématiques, je procédai de la façon suivante : Je fis une table de tous les théorèmes que notre professeur nous avait exposés au

tableau noir; quant aux démonstrations, j'y prêtais fort peu d'attention, mais la chose considérée comme acquise, je me demandais comment je devais m'y prendre pour l'établir d'une façon sûre et irréfutable; un théorème à démontrer était pour moi une sorte de problème d'une espèce particulière à résoudre, dont les éléments de solution se trouvaient dans la table des matières que je possédais par cœur.

Cette façon de procéder m'a gratifié de nombreux défauts, et même d'infirmités assez graves. En général, je ne comprends un Ouvrage de Mathématiques que quand j'en ai moi-même inventé les parties essentielles; jusque-là il est pour moi lettre close. C'est alors seulement que je cherche à me rendre compte des travaux de mes prédécesseurs, à les traduire dans mon système, et à les analyser métaphysiquement.

Dans mes recherches personnelles, je m'efforce de produire les faits les plus variés; je les observe avec le plus grand soin et cherche à me rendre compte de leur raison d'existence.

Si j'y parviens, ils cessent de m'intéresser, et, la plupart du temps, je les oublie et cherche un nouveau sujet sur lequel je puisse exercer ma faculté d'invention, pour l'empêcher de s'atrophier dans l'inaction. Cette manière de procéder me donne des résultats déplorables, je réinvente bien souvent les mêmes choses, mes travaux sont sans suite, sans ordre, avec de nombreuses répétitions.

Peut-être a-t-elle un avantage appréciable, c'est d'attaquer le même sujet à un grand nombre de points de vue différents, parmi lesquels il y en a de préférables que j'adopte en abandonnant les autres.

Ainsi mes espaces résolvants ont précédé mes espaces décomposants dont ils ne sont qu'un cas particulier ([1]).

Une variété de procédés engendre bien souvent une méthode, et des premiers à la seconde il y a loin.

([1]) *Voir* ci-après Chapitre V.

Taine, dans son Étude sur l'intelligence, soutient que les monographies de monstruosités sont ce qu'il y a de plus instructif en psychologie, que pour bien comprendre le mécanisme d'une horloge, il faut voir cette horloge dérangée.

J'aurais, à cet égard, fait un excellent sujet d'étude; au point de vue des difformités, la nature m'a vraiment gâté.

Né horriblement pied-bot, le côté droit de mon crâne est hypertrophié et le côté gauche atrophié; il est orné à droite, en arrière, en haut d'une éminence assez forte, ce qui fait que je suis visuel, que je pense avec l'hémisphère droit, que de mes mains je suis gaucher, et enfin que j'ai une prédilection sensible pour les paradoxes. Malgré mon âge avancé, ma vue s'est conservée remarquable, elle se maintient assez intégralement, pendant que tout le reste de l'organisme s'atrophie et marche peu à peu vers la décrépitude.

J'ai une prédilection marquée pour tout ce qui tient à la méthode graphique et une phobie violente pour l'Analyse mathématique et ses symboles. Si j'ai une question à étudier, je me demande si la méthode graphique ne pourrait m'en donner la solution; si je lis un Ouvrage de Mathématiques, j'en cherche la traduction graphique; enfin, en tout et pour tout, c'est mon seul et unique moyen de comprendre et de travailler. Peut-être ai-je été poussé dans cette voie par l'étude de la méthode Jacotot qui peut se résumer en deux mots : « Sachez bien une chose et rapportez-y tout le reste. »

La seule compensation que m'ait accordée la nature, est une ténacité remarquable. En général, quoi que ce soit que j'entreprenne, les événements les plus imprévus changent en désastres ce qui, d'après mes calculs, aurait dû aboutir au succès. Dans une pareille lutte, on se bronze ou se brise. Les parties faibles de l'organisme s'atrophient, les parties fortes deviennent chaque jour plus résistantes, jusqu'au moment où l'âge amenant la décrépitude ramène tout au même niveau.

Voici une nouvelle particularité de ma méthode de travail. Lisant divers auteurs qui ont traité la question de la parole inté-

rieure, je me suis demandé si elle était une partie intégrante et forcée de la pensée : je n'ai pas tardé à me convaincre que non, et j'en suis arrivé à cette conclusion, qu'elle est un encombrement qui alourdit le travail mental, et que ce que l'on a de mieux à faire c'est de la jeter par-dessus le bord. Elle n'est en réalité qu'un compagnon parasite que l'on s'accoutume à traîner sans aucune utilité, et avec un peu d'exercice j'en suis arrivé à penser exclusivement en choses. J'emploie en général la vision mentale qui va avec une rapidité inouïe, et quand il s'agit de passer en revue de nombreuses hypothèses et leurs conséquences, cette manière de procéder économise un temps précieux.

Peut-être a-t-elle des inconvénients: le principal consiste à rendre très difficile la traduction des résultats obtenus en langage ordinaire; on voit bien son sujet, on le conçoit avec netteté, mais on ne sait comment s'y prendre pour l'exprimer; on cause avec soi-même sans paroles, on s'hypnotise dans son sujet, se créant ainsi un isolement factice dont il est bien difficile de sortir.

Un des exemples les plus remarquables de cette manière de procéder, est celui des comptables exécutant à l'œil l'addition d'une longue colonne de chiffres avec une rapidité qui tient du prodige. Tout visuel pourrait, je crois, en s'exerçant, arriver à faire ces tours de force. Le secret du truc consiste dans l'élimination absolue de la parole intérieure et l'emploi exclusif de la vision mentale.

Dans mon étude sur les espaces arithmétiques hypermagiques, j'ai appelé l'attention sur les avantages de l'analyse métaphysique; il me semble inutile de me répéter, je m'en sers couramment dans toutes mes études et je puis affirmer qu'elle m'est d'un grand secours.

Il est une chose universellement reconnue aujourd'hui, c'est que les organismes chez lesquels une partie a pris une prédominance exceptionnelle exécutent avec une grande perfection les opérations qui la concernent, et cela naturellement, sans éducation scolaire. Les individus qui les possèdent font eux-mêmes leur éducation sans

s'en douter, et en arrivent à une supériorité que d'autres s'efforceraient bien inutilement d'acquérir; prenez leurs œuvres, analysez-les métaphysiquement, vous possédez la technique de ce genre de travail.

L'analyse métaphysique exécutée, transportez par analogie ces méthodes dans un autre genre, et vous approchez de la perfection.

L'analogie peut se résumer en deux mots. Soit F un genre de combinaisons ou fonctions, soient φ et ψ deux autres fonctions. Si vous faites les fonctions de fonctions $F\varphi$ et $F\psi$, il existe entre elles une analogie qui est F.

La fonction combinante est indépendante des fonctions combinées; si, par l'analyse métaphysique vous parvenez à l'isoler, vous pouvez ensuite l'appliquer à n'importe quelle autre fonction, de n'importe quel genre.

Au fond, ce que l'on appelle l'*abstraction* n'est pas autre chose. Tout concret est une fonction de fonction $F\varphi$; dégagez F, vous avez fait une abstraction, vous avez un abstrait.

On a beaucoup médit des *entités;* au fond, *il n'existe dans la nature que des entités,* c'est-à-dire des combinaisons de constances et de variations; les constances constituent à proprement dire les entités.

Et même en Mathématiques, ce que l'on nomme des *propriétés,* ne sont autre chose que des constances. Une considération possède une propriété, parce que la fonction plus ou moins complexe qui la constitue, qui est sa raison d'existence, possède des constances. Mon but dans cette préface n'étant que d'effleurer la question, je dois m'abstenir de la développer, et je passe à un autre sujet.

Parmi toutes ses œuvres, celle que Descartes a le plus estimée, c'est sa *Regulæ ad directionen ingenii* que Leibniz fit copier avec soin et qu'il intitula : *De inquirendi veritate.*

C'est là une étude de psychologie et métaphysique positives aussi avancée que pouvaient le permettre les connaissances de l'époque. Depuis lors la psychologie et la spécieuse ont fait des progrès con-

sidérables, et il y aurait certainement lieu de mettre cette importante question au niveau des connaissances actuelles.

Viète, en inventant la spécieuse dans son *Introduction à l'art analytique,* avait la singulière prétention *nullum non problema solvere*. Ses successeurs les mathématiciens analystes ont renchéri encore, et la plupart d'entre eux disent nettement qu'il faut, dans toute recherche, éliminer absolument le concret et ramener tout à des combinaisons de symboles ayant certaines propriétés, que l'on arrive à manipuler suivant des règles fixes, et par suite mécaniques. Vous avez une question à résoudre, vous la posez en symboles. Vous manipulez ces derniers conformément aux règles de l'art, et la conclusion atteinte, vous faites la traduction inverse. A quoi correspondent les combinaisons symboliques intermédiaires? Que vous importe! Vous vouliez un résultat, une solution, la voilà. C'est tout ce que vous pouvez demander.

Certains auteurs métaphysiciens ne sont pas complètement de cet avis. Quelques-uns, peu révérencieux, prétendent qu'au point de vue de l'invention, les résultats sont nuls, que l'analyse est un moulin qui moud admirablement le blé que l'on a jeté dans la trémie, et rend, bien bluté en son et farine, *ce que vous y avez mis*, *et rien de plus*.

Poinsot dans sa théorie nouvelle de la rotation des corps dit :

« Ce n'est point dans le calcul que réside *cet art qui nous fait découvrir,* mais dans cette considération attentive des choses où l'esprit cherche avant tout à s'en faire une idée en essayant par l'*Analyse proprement dite* de les décomposer en d'autres plus simples afin de les revoir ensuite comme si elles étaient formées par la réunion de ces choses simples dont il a une pleine connaissance. Ce n'est pas que les choses soient composées de cette manière, mais c'est notre seule manière de les voir, de nous en faire une idée, et partant de les connaître. Ainsi notre vraie méthode n'est que cet heureux mélange de l'*analyse* et de la synthèse, *où le calcul n'est employé que comme instrument, instrument précieux et nécessaire sans doute parce qu'il assure et facilite*

notre marche, mais qui n'a par lui-même aucune vertu propre, qui ne dirige point l'esprit, mais que l'esprit doit diriger comme tout instrument. »

Et Chasles termine ainsi son discours d'inauguration du Cours de Géométrie supérieure :

« On reconnaît ici quels sont les avantages propres de l'Analyse et de la Géométrie. La première, par le mécanisme merveilleux de ses transformations, passe rapidement du point de départ au but proposé, *mais souvent sans connaître ni le chemin qu'elle a fait, ni la signification des nombreuses formules qu'elle a employées.*

» La Géométrie, au contraire, *qui ne puise ses inspirations que dans la considération attentive des choses et dans l'enchaînement des idées,* est obligée de découvrir naturellement les propositions que l'Analyse a pu négliger et ignorer *et qui forment le lien le plus immédiat entre les deux extrêmes.*

» Cette marche peut paraître parfois difficile, mais elle est au fond la plus simple parce qu'elle est la plus directe; *elle est aussi la plus lumineuse et la plus féconde.*

» L'Analyse découvre-t-elle une vérité, que la Géométrie en cherche la démonstration par ses propres moyens : soyez sûr que dans cette recherche elle rencontrera et fera connaître diverses autres propriétés qui se rattachent au sujet, l'éclairent et le complètent.

» L'Analyse et la Géométrie *au point de vue philosophique* sont deux branches d'une science unique qui a pour objet la recherche des vérités naturelles; elles sont destinées à s'éclairer naturellement et à se prêter un secours réciproque : toutes deux sont des instruments aujourd'hui indispensables. »

Dans sa préface, Chasles résume sa manière de concevoir les *imaginaires*. Elle est trop remarquable pour que je puisse la passer sous silence dans un livre qui a principalement pour but de montrer ce que sont les imaginaires en Arithmétique.

« Une étude attentive des différents procédés de démonstration qui peuvent s'appliquer à une même question m'a montré qu'à côté d'une démonstration facile, fondée sur quelques propriétés *accidentelles et contingentes* d'une figure, devaient toujours s'en trouver d'autres, fondées sur *des propriétés absolues* et subsistant dans tous les cas que peut présenter la figure en raison de la diversité de position de ses parties; et j'ai éprouvé que la recherche de ces démonstrations complètement rigoureuses est d'autant plus utile, qu'elle met nécessairement sur la voie des propositions les plus importantes, *de celles qui établissent tous les liens qui doivent exister entre les différentes parties d'un même sujet.*

» Je me suis donc proposé d'introduire dans cet Ouvrage, *avec la notion explicite des imaginaires*, des démonstrations aussi rigoureuses et aussi générales que celles de la Géométrie analytique.

» Ces démonstrations deviennent aussi faciles que les premières quand on en a préparé la voie par la recherche *de quelques propositions d'une certaine nature, savoir des propositions reposant sur les propriétés absolues et permanentes de la figure que l'on considère, et non simplement sur ses propriétés contingentes.* Ces propositions se distinguent par ce caractère spécial *que les objets susceptibles de devenir imaginaires n'y entrent pas sous forme explicite, mais s'y trouvent représentés par des éléments réels,* de même que les racines d'une équation n'entrent pas elles-mêmes dans les calculs de la Géométrie analytique et y sont représentés collectivement par les coefficients de l'équation.

» Ces propositions où n'entrent ainsi que des relations *qui, en Analyse, s'exprimeraient au moyen des coefficients d'une équation ou d'autres fonctions symétriques des racines* de l'équation, sont celles qu'il importe le plus de connaître, comme étant à la fois les plus fécondes et les plus propres à donner à la Géométrie le degré de généralité qui fait la puissance de l'Analyse.

» Je terminerai ces considérations sur les *imaginaires* par une remarque qui se rapporte essentiellement au sujet.

» Il peut arriver, quand les parties d'une figure deviennent imagi-

naires, que les propositions soient susceptibles de nouveaux énoncés très différents des premiers, et donnent lieu à des propositions de l'étendue très différentes de celles que l'on considérait d'abord.

» On trouvera un exemple d'une telle transformation dans un système de cercles ayant le même axe radical. Si l'on suppose l'un des cercles imaginaires, ce qui aura lieu selon la position du point que l'on prendra pour centre du cercle, toutes les propositions générales appartenant à ce système *fournissent immédiatement, en changeant d'énoncés, de fort belles propriétés des cônes à base circulaire.* »

Ne voulant ici qu'effleurer cette question, je cesserai de suivre Chasles dans sa manière d'interpréter les imaginaires. Pourtant le lecteur peut se rendre compte de certaines analogies. Les parties réelles sont ici, comme dans les fonctions arithmétiques, *des fonctions symétriques des imaginaires,* et la fin de l'extrait ci-dessus en arrive à *considérer le réel comme un cas particulier de l'imaginaire.*

Il y aurait certainement un travail intéressant à faire, qui consisterait à *systématiser ce que,* dans les diverses études que l'on peut faire, *on entend par imaginaires;* car au fond de toutes ces considérations *contingentes,* comme dit Chasles, on trouverait certainement d'autres considérations fondamentales *permanentes et absolues* qui constitueraient *la notion métaphysique de l'imaginaire prise en elle-même et abstraction faite de toute application spéciale.*

Il y aurait encore beaucoup de choses à dire sur ces questions de psychologie et de métaphysique positives, mais cela m'entraînerait beaucoup trop loin de mon sujet. Je m'arrête donc et passe la parole à mon collaborateur.



ARITHMÉTIQUE GRAPHIQUE.

INTRODUCTION A L'ÉTUDE DES FONCTIONS ARITHMÉTIQUES.

INTRODUCTION.

1. On appelle *fonction arithmétique* une fonction algébrique $f(x, y, z, \ldots)$ dans laquelle les variables x, y, z ne peuvent être que des nombres entiers. Cette fonction est donc par nature discontinue, et l'étude des fonctions arithmétiques se distinguera essentiellement de celle des fonctions de l'Algèbre, où les variables reçoivent en général toutes les valeurs possibles.

En particulier la fonction $f(x, y, z, \ldots)$ peut être un polynome à coefficients entiers. En outre, le nombre des variables peut être quelconque. Dans la présente étude, nous ne nous occuperons que des polynomes $f(x)$ à une seule variable et à coefficients entiers. Il est donc bien entendu que, dans tout ce qui va suivre, l'expression *fonction arithmétique* devra être prise sous cette acception restreinte, chaque fois que nous l'emploierons, sans qu'il soit nécessaire de le répéter.

2. Dans toute étude concernant les fonctions arithmétiques, on



se trouvera conduit à des égalités de la forme $f(x) = \varphi(x)$, auxquelles il est essentiel de s'arrêter pour en bien préciser le sens, qui n'est pas le même qu'en Algèbre. Gauss a donné à toute égalité de cette nature le nom de *congruence*, et, écrivant

$$a \equiv b \pmod{m},$$

il entend par là que les nombres a et b étant divisés par un nombre m appelé *module*, et du reste choisi à volonté, donneront le même reste.

Poinsot, dans un Mémoire lu à l'Académie des Sciences le 5 mai 1817, et Galois, dans une Note *Sur la théorie des nombres* (*Œuvres*, p. 15), proposent de regarder par convention le module m comme nul, ainsi que tous ses multiples, et de traiter dès lors la congruence comme une simple égalité ordinaire $a = b$.

C'est à ce point de vue de Poinsot et de Galois que nous nous placerons invariablement. Au fond, cela revient à une convention en vertu de laquelle on considère toujours le module comme nul, tandis que la conception de Gauss repose sur la notion de divisibilité. Les deux idées ne sont pas opposées l'une à l'autre; on pourrait même dire qu'elles sont identiques; mais la forme sous laquelle elles se présentent est fort différente; et il y a selon nous de tels avantages à celle que nous adoptons, ne fût-ce que dans la simplicité des écritures et des raisonnements, que nulle hésitation n'est permise.

3. Une autre considération fondamentale pour l'objet qui nous occupe, et que nous empruntons également à Galois, est celle des imaginaires arithmétiques, définies par lui comme des solutions de congruences impossibles en nombres entiers, et dont les propriétés importantes tendent à créer une analogie plus étroite entre les équations arithmétiques et les équations algébriques. Il y a en effet entre ces deux domaines des rapprochements fréquents, et aussi des dissemblances tenant à la nature des choses.

Ce n'est pas sans quelque hésitation que nous avons conservé, faute de mieux, ce terme d'*imaginaire*, qui s'applique ici à des objets tout à fait différents des imaginaires de l'Algèbre, lesquelles sont invariablement de la forme $a + b\sqrt{-1}$. Mais aucune équi-

voque ne pourra se produire si l'on veut bien prendre la peine de nous suivre avec un peu d'attention dans nos développements et, dès maintenant, nous croyons nécessaire de proclamer la distinction capitale à établir entre les imaginaires algébriques et les *imaginaires arithmétiques*.

Dès le début on verra apparaître des imaginaires arithmétiques dans la théorie des Tables de division, et nous espérons montrer avec une entière clarté comment ces diverses sortes d'imaginaires se relient les unes aux autres, et comment elles proviennent en réalité d'une cause unique, qui est l'impossibilité de certaines opérations. En supposant que le résultat soit alors représentable par un symbole conventionnel, on élargit le champ de la Science, on lui donne une plus grande généralité et l'on renverse des obstacles qui semblaient devoir nous arrêter dans notre route. C'est ce qui se produit, comme on le sait, en Algèbre; c'est ce qui a lieu aussi en Arithmétique.

4. A l'étude qui fait l'objet de ce livre s'appliquent heureusement et simplement les méthodes exposées dans notre Ouvrage précédent, *Les espaces arithmétiques hypermagiques,* publié en 1894 et précédé du titre général *Arithmétique graphique* que nous avons conservé. Nous ne saurions recommencer à présenter l'exposé de ces méthodes et les définitions nécessaires à leur complète intelligence. Aussi nous arrivera-t-il de renvoyer quelquefois à l'Ouvrage en question en l'indiquant par la notation entre parenthèses (*Esp. ar.*).

Les titres des Chapitres qui suivent indiqueront suffisamment la nature des matières qui s'y trouveront traitées. On remarquera que nous avons tenu à présenter tout d'abord l'exposé des opérations élémentaires, multiplication, division, formation des puissances et extraction des racines, portant exclusivement sur des entiers.

D'assez nombreuses figures sont nécessaires pour suivre utilement les développements d'une méthode essentiellement graphique. Nous prions le lecteur d'y porter toute son attention. Ce ne sont pas de simples illustrations sur des exemples; le plus souvent on y verra au contraire de véritables démonstrations par les faits, démonstrations ayant souvent le mérite de montrer non seulement

comment certaines propriétés se révèlent, mais encore pourquoi elles existent.

Une grande partie des considérations qui font l'objet du présent Ouvrage ont été exposées successivement dans des Mémoires publiés par nous dans les comptes rendus des Congrès de l'*Association française pour l'avancement des Sciences*, années 1900, 1901, 1902, 1903, 1904. D'autres au contraire sont nouvelles, et le tout forme un ensemble auquel nous nous sommes efforcé de donner de l'unité.

CHAPITRE PREMIER.

MULTIPLICATION ET DIVISION DES ENTIERS.

Espaces modulaires.

5. Une série de points équidistants sur une droite, ou une ligne de cases carrées égales juxtaposées, forme un espace arithmétique à une dimension.

Une juxtaposition d'espaces à une dimension, placés les uns à côté des autres, forme un espace à deux dimensions, et ainsi de suite. On peut considérer ainsi des espaces à autant de dimensions que l'on voudra.

Chacun de ces espaces peut être fini ou indéfini. Si, ayant fait une opération graphique quelconque sur un espace à une dimension, par exemple, il nous convient de n'en considérer le résultat que par rapport à un certain module m, nous pouvons sectionner notre espace indéfini en files de m cases chacune, à partir d'une case prise pour origine, et superposer toutes ces files en une seule, de m cases, qui nous offrira l'image de ce qui se passe indéfiniment, sur l'espace primitivement considéré. Nous aurons ainsi construit l'espace modulaire à une dimension, de module m.

En associant m espaces modulaires de module m par juxtaposition, nous aurons un carré de m^2 cases, espace modulaire à deux dimensions; de même, nous obtiendrons un cube de m^3 cases, espace modulaire à trois dimensions, un espace modulaire à quatre dimensions, contenant m^4 cases, et ainsi de suite (*Esp. ar.*, p. 13-17).

Dans ces espaces congruents, on peut considérer des lignes régulières, et des directions, parallèles à ces lignes, en marchant d'un pas régulier à partir d'une case déterminée, pour aboutir à une

autre case aussi déterminée, et continuant ainsi indéfiniment (*Esp. ar.*, p. 25, 30-31).

6. Tous les développements qui vont suivre ont trait à un calcul de congruences, ou modulaire. Le module étant m, toutes les données et les résultats, en nombres entiers, seront donc compris dans la suite des termes 0, 1, 2, 3, ..., $m-1$, que nous appellerons les *chiffres* relatifs à m. Un chiffre *quelconque* sera souvent désigné par la notation $((m))$ (*Esp. ar.*, p. 19).

Multiplication.

7. Plusieurs nombres a, b, c, ... étant donnés, si l'on veut former leur produit, on devra les remplacer par leurs chiffres correspondants α, β, γ, ..., auxquels ils sont modulairement égaux; puis il s'agira de déterminer le chiffre égal à $\alpha\beta\gamma...$, lequel sera le produit $abc...$. On pourra dans ce but procéder par multiplications successives, et par suite on sera ramené à effectuer des produits de deux facteurs seulement. Une Table de multiplication nous sera fournie par un espace modulaire de m^2 cases, les deux coordonnées de chaque case correspondant à des arguments représentés par les deux facteurs, et cette figure résoudra complètement le problème. Nous donnons ici (*fig.* 1, 3, 5, 7) quatre exemples de Tables de multiplication, correspondant aux modules 11, 9, 15, 12. La construction de ces Tables devra se faire par l'addition successive de chaque ligne avec la première, ou, ce qui revient au même, on écrira sur chaque ligne d'argument α les chiffres rencontrés par une marche de pas α sur l'espace linéaire 0, 1, 2, ..., $m-1$. Il s'ensuit, pour un module premier, que toutes les lignes contiennent tous les chiffres; cela n'a lieu au contraire, dans le cas d'un module composé, que pour les lignes qui correspondent à un argument premier avec le module.

On remarquera que la Table de multiplication, quel que soit le module, est symétrique par rapport à la diagonale partant de l'origine. En outre, la dernière ligne (et par suite la dernière colonne) contient les chiffres 1, 2, ..., $m-1$ dans leur ordre inverse, ce

qui résulte de l'identité modulaire

$$\alpha(m-1) = m - \alpha.$$

La diagonale partant de l'origine contient les seuls chiffres qui soient des carrés, par rapport au module. Ce sont ces nombres qu'on désigne souvent sous le nom bien compliqué de *résidus quadratiques*. La suite de ces carrés sur la diagonale est symétrique, car

$$\alpha^2 = (m-\alpha)^2.$$

Il y a fréquemment avantage, pour la simplification de l'écriture, à employer des chiffres négatifs; cela permet souvent même de mieux faire ressortir certaines propriétés. Nous avons procédé ainsi dans les figures 5 et 7, où nous écrivons

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ \bar{7}\ \bar{6}\ \bar{5}\ \bar{4}\ \bar{3}\ \bar{2}\ \bar{1}$$

au lieu de

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14,$$

et

$$1\ 2\ 3\ 4\ 5\ 6\ \bar{5}\ \bar{4}\ \bar{3}\ \bar{2}\ \bar{1}$$

au lieu de

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11.$$

8. On pourrait imaginer la représentation des produits de trois facteurs par un cube modulaire analogue, et en général celle des produits de n facteurs par un espace modulaire à n dimensions. Cela n'offrirait pas d'intérêt pratique, mais il peut être intéressant de constater que dans ces divers espaces les m chiffres de la diagonale principale représenteraient respectivement les cubes, les bicarrés, etc., par rapport au module, ou, si l'on veut, les résidus cubiques, biquadratiques, etc.

Division.

9. La division étant l'opération inverse de la multiplication, il est facile et utile de former, au moyen des Tables de multiplication, des Tables de division ayant pour arguments le

dividende D (première ligne du cadre dans les figures) et le diviseur *d* (première colonne du cadre); dans chaque case ainsi déterminée est inscrit le quotient correspondant. Nous donnons ici des Tables de division (*fig.* 2, 4, 6, 8) pour les modules 11, 9, 15, 12, en regard des Tables de multiplication correspondantes.

Table de multiplication, module 11.

Fig. 1.

	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Table de division, module 11.

Fig. 2.

d

D	0	1	2	3	4	5	6	7	8	9	10
0	0, ... .10										
1	0	1	2	3	4	5	6	7	8	9	10
2	0	6	1	7	2	8	3	9	4	10	5
3	0	4	8	1	5	9	2	6	10	3	7
4	0	3	6	9	1	4	7	10	2	5	8
5	0	9	7	5	3	1	10	8	6	4	2
6	0	2	4	6	8	10	1	3	5	7	9
7	0	8	5	2	10	7	4	1	9	6	3
8	0	7	3	10	6	2	9	5	1	8	4
9	0	5	10	4	9	3	8	2	7	1	6
10	0	10	9	8	7	6	5	4	3	2	1

Table de multiplication, module 9.

Fig. 3.

	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Table de division, module 9.

Fig. 4.

d \ D	0	1	2	3	4	5	6	7	8
0	0, ..., ..., 8								
1	0	1	2	3	4	5	6	7	8
2	0	5	1	6	2	7	3	8	4
3	0, 3 6			1, 4 7			2. 5 8		
4	0	7	5	3	1	8	6	4	2
5	0	2	4	6	8	1	3	5	7
6	0. 3 6			2, 5 8			1, 4 7		
7	0	4	8	3	7	2	6	1	5
8	0	8	7	6	5	4	3	2	1

Table de multiplication, module 15.

Fig. 5.

	0	1	2	3	4	5	6	7	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
2	0	2	4	6	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	1	3	5	7	$\bar{6}$	$\bar{4}$	$\bar{2}$
3	0	3	6	$\bar{6}$	$\bar{3}$	0	3	6	$\bar{6}$	$\bar{3}$	0	3	6	$\bar{6}$	$\bar{3}$
4	0	4	$\bar{7}$	$\bar{3}$	1	5	$\bar{6}$	$\bar{2}$	2	6	$\bar{5}$	$\bar{1}$	3	7	$\bar{4}$
5	0	5	$\bar{5}$	0	5	$\bar{5}$	0	5	$\bar{5}$	0	5	$\bar{5}$	0	5	$\bar{5}$
6	0	6	$\bar{3}$	3	$\bar{6}$	0	6	$\bar{3}$	3	$\bar{6}$	0	6	$\bar{3}$	3	$\bar{6}$
7	0	7	$\bar{1}$	6	$\bar{2}$	5	$\bar{3}$	4	$\bar{4}$	3	$\bar{5}$	2	$\bar{6}$	1	$\bar{7}$
$\bar{7}$	0	$\bar{7}$	1	$\bar{6}$	2	$\bar{5}$	3	$\bar{4}$	4	$\bar{3}$	5	$\bar{2}$	6	$\bar{1}$	7
$\bar{6}$	0	$\bar{6}$	3	$\bar{3}$	6	0	$\bar{6}$	3	$\bar{3}$	6	0	$\bar{6}$	3	$\bar{3}$	6
$\bar{5}$	0	$\bar{5}$	5	0	$\bar{5}$	5	0	$\bar{5}$	5	0	$\bar{5}$	5	0	$\bar{5}$	5
$\bar{4}$	0	$\bar{4}$	7	3	$\bar{1}$	$\bar{5}$	6	2	$\bar{2}$	$\bar{6}$	5	1	$\bar{3}$	$\bar{7}$	4
$\bar{3}$	0	$\bar{3}$	$\bar{6}$	6	3	0	$\bar{3}$	$\bar{6}$	6	3	0	$\bar{3}$	$\bar{6}$	6	3
$\bar{2}$	0	$\bar{2}$	$\bar{4}$	$\bar{6}$	7	5	3	1	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$	6	4	2
$\bar{1}$	0	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	7	6	5	4	3	2	1

Table de division, module 15.

Fig. 6.

d

	0	1	2	3	4	5	6	7	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
0	0. 1, ... $\bar{1}$														
1	0	1	2	3	4	5	6	7	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
2	0	$\bar{7}$	1	$\bar{6}$	2	$\bar{5}$	3	$\bar{4}$	4	$\bar{3}$	5	$\bar{2}$	6	$\bar{1}$	7
3	0. 5 $\bar{5}$			1, 6 $\bar{4}$			2, 7 $\bar{3}$			3. $\bar{7}$ $\bar{2}$			4. $\bar{6}$ $\bar{1}$		
4	0	4	$\bar{7}$	$\bar{3}$	1	5	$\bar{6}$	$\bar{2}$	2	6	$\bar{5}$	$\bar{1}$	3	7	$\bar{4}$
5	0. 3. 6 $\bar{6}$, $\bar{3}$					1. 4 7 $\bar{5}$, $\bar{2}$					2, 5, $\bar{7}$ $\bar{4}$, $\bar{1}$				
6	0. 5 $\bar{5}$			3, $\bar{7}$ $\bar{2}$			1, 6 $\bar{4}$			4. $\bar{6}$ $\bar{1}$			2. 7 $\bar{3}$		
7	0	$\bar{2}$	$\bar{4}$	$\bar{6}$	7	5	3	1	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$	6	4	2
$\bar{7}$	0	2	4	6	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	1	3	5	7	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	0. 5 $\bar{5}$			2. 7 $\bar{3}$			4. $\bar{6}$ $\bar{1}$			1. 6 $\bar{4}$			3, $\bar{7}$ $\bar{2}$		
$\bar{5}$	0, 3. 6 $\bar{6}$, $\bar{3}$					2, 5, $\bar{7}$ $\bar{4}$, $\bar{1}$					1, 4. 7 $\bar{5}$, $\bar{2}$				
$\bar{4}$	0	$\bar{4}$	7	3	$\bar{1}$	$\bar{5}$	6	2	$\bar{2}$	$\bar{6}$	5	1	$\bar{3}$	$\bar{7}$	4
$\bar{3}$	0. 5 $\bar{5}$			4, $\bar{6}$ $\bar{1}$			3, $\bar{7}$ $\bar{2}$			2. 7 $\bar{3}$			1. 6 $\bar{4}$		
$\bar{2}$	0	7	$\bar{1}$	6	$\bar{2}$	5	$\bar{3}$	4	$\bar{4}$	3	$\bar{5}$	2	$\bar{6}$	1	$\bar{7}$
$\bar{1}$	0	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	7	6	5	4	3	2	1

Table de multiplication, module 12.

Fig. 7.

	0	1	2	3	4	5	6	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
2	0	2	4	6	$\bar{4}$	$\bar{2}$	0	2	4	6	$\bar{4}$	$\bar{2}$
3	0	3	6	$\bar{3}$	0	3	6	$\bar{3}$	0	3	6	$\bar{3}$
4	0	4	$\bar{4}$	0	4	$\bar{4}$	0	4	$\bar{4}$	0	4	$\bar{4}$
5	0	5	$\bar{2}$	3	$\bar{4}$	1	6	$\bar{1}$	4	$\bar{3}$	2	$\bar{5}$
6	0	6	0	6	0	6	0	6	0	6	0	6
$\bar{5}$	0	$\bar{5}$	2	$\bar{3}$	4	$\bar{1}$	6	1	$\bar{4}$	3	$\bar{2}$	5
$\bar{4}$	0	$\bar{4}$	4	0	$\bar{4}$	4	0	$\bar{4}$	4	0	$\bar{4}$	4
$\bar{3}$	0	$\bar{3}$	6	3	0	$\bar{3}$	6	3	0	$\bar{3}$	6	3
$\bar{2}$	0	$\bar{2}$	$\bar{4}$	6	4	2	0	$\bar{2}$	$\bar{4}$	6	4	2
$\bar{1}$	0	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	6	5	4	3	2	1

Table de division, module 12.

Fig. 8.

d

D	0	1	2	3	4	5	6	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
0	0, ..., $\bar{1}$											
1	0	1	2	3	4	5	6	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
2	0. 6		1, $\bar{5}$		2. $\bar{4}$		3, $\bar{3}$		4, $\bar{2}$		5, $\bar{1}$	
3	0, 4 $\bar{4}$			1. 5 $\bar{3}$			2, 6 $\bar{2}$			3, $\bar{5}$ $\bar{1}$		
4	0, 3 6, $\bar{3}$				1, 4 $\bar{5}$, $\bar{2}$				2, 5 $\bar{4}$, $\bar{1}$			
5	0	5	$\bar{2}$	3	$\bar{4}$	1	6	$\bar{1}$	4	$\bar{3}$	2	$\bar{5}$
6	0, 2, 4 6, $\bar{4}$, $\bar{2}$						1, 3, 5 $\bar{5}$, $\bar{3}$, $\bar{1}$					
$\bar{5}$	0	$\bar{5}$	2	$\bar{3}$	4	$\bar{1}$	6	1	$\bar{4}$	3	$\bar{2}$	5
$\bar{4}$	0, 3 6, $\bar{3}$				2, 5 $\bar{4}$, $\bar{1}$				1, 4 $\bar{5}$, $\bar{2}$			
$\bar{3}$	0, 4 $\bar{4}$			3, $\bar{5}$ $\bar{1}$			2, 6 $\bar{2}$			1, 5 $\bar{3}$		
$\bar{2}$	0. 6		5. $\bar{1}$		4, $\bar{2}$		3, $\bar{3}$		2, $\bar{4}$		1. $\bar{5}$	
$\bar{1}$	0	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	6	5	4	3	2	1

Table de multiplication, module 15.

Fig. 5.

	0	1	2	3	4	5	6	7	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
2	0	2	4	6	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	1	3	5	7	$\bar{6}$	$\bar{4}$	$\bar{2}$
3	0	3	6	$\bar{6}$	$\bar{3}$	0	3	6	$\bar{6}$	$\bar{3}$	0	3	6	$\bar{6}$	$\bar{3}$
4	0	4	$\bar{7}$	$\bar{3}$	1	5	$\bar{6}$	$\bar{2}$	2	6	$\bar{5}$	$\bar{1}$	3	7	$\bar{4}$
5	0	5	$\bar{5}$	0	5	$\bar{5}$	0	5	$\bar{5}$	0	5	$\bar{5}$	0	5	$\bar{5}$
6	0	6	$\bar{3}$	3	$\bar{6}$	0	6	$\bar{3}$	3	$\bar{6}$	0	6	$\bar{3}$	3	$\bar{6}$
7	0	7	$\bar{1}$	6	$\bar{2}$	5	$\bar{3}$	4	$\bar{4}$	3	$\bar{5}$	2	$\bar{6}$	1	$\bar{7}$
$\bar{7}$	0	$\bar{7}$	1	$\bar{6}$	2	$\bar{5}$	3	$\bar{4}$	4	$\bar{3}$	5	$\bar{2}$	6	$\bar{1}$	7
$\bar{6}$	0	$\bar{6}$	3	$\bar{3}$	6	0	$\bar{6}$	3	$\bar{3}$	6	0	$\bar{6}$	3	$\bar{3}$	6
$\bar{5}$	0	$\bar{5}$	5	0	$\bar{5}$	5	0	$\bar{5}$	5	0	$\bar{5}$	5	0	$\bar{5}$	5
$\bar{4}$	0	$\bar{4}$	7	3	$\bar{1}$	$\bar{5}$	6	2	$\bar{2}$	$\bar{6}$	5	1	$\bar{3}$	$\bar{7}$	4
$\bar{3}$	0	$\bar{3}$	$\bar{6}$	6	3	0	$\bar{3}$	$\bar{6}$	6	3	0	$\bar{3}$	$\bar{6}$	6	3
$\bar{2}$	0	$\bar{2}$	$\bar{4}$	$\bar{6}$	7	5	3	1	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$	6	4	2
$\bar{1}$	0	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	7	6	5	4	3	2	1

Table de division, module 15.

Fig. 6.

d	0	1	2	3	4	5	6	7	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
0	0.1,.... ... $\bar{1}$														
1	0	1	2	3	4	5	6	7	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
2	0	$\bar{7}$	1	$\bar{6}$	2	$\bar{5}$	3	$\bar{4}$	4	$\bar{3}$	5	$\bar{2}$	6	$\bar{1}$	7
3	0, 5 $\bar{5}$			1, 6 $\bar{4}$			2, 7 $\bar{3}$			3, $\bar{7}$ $\bar{2}$			4, $\bar{6}$ $\bar{1}$		
4	0	4	$\bar{7}$	$\bar{3}$	1	5	$\bar{6}$	$\bar{2}$	2	6	$\bar{5}$	$\bar{1}$	3	7	$\bar{4}$
5	0, 3, 6 $\bar{6}$, $\bar{3}$					1, 4 7 $\bar{5}$, $\bar{2}$					2, 5, $\bar{7}$ $\bar{4}$, $\bar{1}$				
6	0, 5 $\bar{5}$			3, $\bar{7}$ $\bar{2}$			1, 6 $\bar{4}$			4, $\bar{6}$ $\bar{1}$			2, 7 $\bar{3}$		
7	0	$\bar{2}$	$\bar{4}$	$\bar{6}$	7	5	3	1	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$	6	4	2
$\bar{7}$	0	2	4	6	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	1	3	5	7	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	0, 5 $\bar{5}$			2, 7 $\bar{3}$			4, $\bar{6}$ $\bar{1}$			1, 6 $\bar{4}$			3, $\bar{7}$ $\bar{2}$		
$\bar{5}$	0, 3, 6 $\bar{6}$, $\bar{3}$					2, 5, $\bar{7}$ $\bar{4}$, $\bar{1}$					1, 4, 7 $\bar{5}$, $\bar{2}$				
$\bar{4}$	0	$\bar{4}$	7	3	$\bar{1}$	$\bar{5}$	6	2	$\bar{2}$	$\bar{6}$	5	1	$\bar{3}$	$\bar{7}$	4
$\bar{3}$	0, 5 $\bar{5}$			4, $\bar{6}$ $\bar{1}$			3, $\bar{7}$ $\bar{2}$			2, 7 $\bar{3}$			1, 6 $\bar{4}$		
$\bar{2}$	0	7	$\bar{1}$	6	$\bar{2}$	5	$\bar{3}$	4	$\bar{4}$	3	$\bar{5}$	2	$\bar{6}$	1	$\bar{7}$
$\bar{1}$	0	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	7	6	5	4	3	2	1

Table de multiplication, module 12.

Fig. 7.

	0	1	2	3	4	5	6	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
2	0	2	4	6	$\bar{4}$	$\bar{2}$	0	2	4	6	$\bar{4}$	$\bar{2}$
3	0	3	6	$\bar{3}$	0	3	6	$\bar{3}$	0	3	6	$\bar{3}$
4	0	4	$\bar{4}$	0	4	$\bar{4}$	0	4	$\bar{4}$	0	4	$\bar{4}$
5	0	5	$\bar{2}$	3	$\bar{4}$	1	6	$\bar{1}$	4	$\bar{3}$	2	$\bar{5}$
6	0	6	0	6	0	6	0	6	0	6	0	6
$\bar{5}$	0	$\bar{5}$	2	$\bar{3}$	4	$\bar{1}$	6	1	$\bar{4}$	3	$\bar{2}$	5
$\bar{4}$	0	$\bar{4}$	4	0	$\bar{4}$	4	0	$\bar{4}$	4	0	$\bar{4}$	4
$\bar{3}$	0	$\bar{3}$	6	3	0	$\bar{3}$	6	3	0	$\bar{3}$	6	3
$\bar{2}$	0	$\bar{2}$	$\bar{4}$	6	4	2	0	$\bar{2}$	$\bar{4}$	6	4	2
$\bar{1}$	0	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	6	5	4	3	2	1

Table de division, module 12.

Fig. 8.

D \ *d*	0	1	2	3	4	5	6	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
0	0, …, $\bar{1}$											
1	0	1	2	3	4	5	6	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
2	0. 6		1, $\bar{5}$		2. $\bar{4}$		3, $\bar{3}$		4, $\bar{2}$		5. $\bar{1}$	
3	0. 4 $\bar{4}$			1. 5 $\bar{3}$			2. 6 $\bar{2}$			3, $\bar{5}$ $\bar{1}$		
4	0, 3 6, $\bar{3}$				1. 4 $\bar{5}$, $\bar{2}$				2, 5 $\bar{4}$, $\bar{1}$			
5	0	5	$\bar{2}$	3	$\bar{4}$	1	6	$\bar{1}$	4	$\bar{3}$	2	$\bar{5}$
6	0, 2, 4 6, $\bar{4}$, $\bar{2}$						1, 3, 5 $\bar{5}$, $\bar{3}$, $\bar{1}$					
$\bar{5}$	0	$\bar{5}$	2	$\bar{3}$	4	$\bar{1}$	6	1	$\bar{4}$	3	$\bar{2}$	5
$\bar{4}$	0, 3 6. $\bar{3}$				2, 5 $\bar{4}$. $\bar{1}$				1, 4 $\bar{5}$, $\bar{2}$			
$\bar{3}$	0, 4 $\bar{4}$			3. $\bar{5}$ $\bar{1}$			2, 6 $\bar{2}$			1, 5 $\bar{3}$		
$\bar{2}$	0. 6		5. $\bar{1}$		4, $\bar{2}$		3, $\bar{3}$		2, $\bar{4}$		1. $\bar{5}$	
$\bar{1}$	0	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	6	5	4	3	2	1

La différence entre la Table de module 11 et les trois autres est profonde; dans la première, toutes les cases sont remplies, sauf dans la première ligne; dans les autres, certaines cases restent vides, et d'autres contiennent plusieurs chiffres. Cela tient à ce que le module 11 est premier, tandis que les trois autres 9, 15, 12 sont composés, et respectivement, des formes a^α, ab, $a^\alpha b$. On remarquera que les cases vides apparaissent toujours dans les lignes des diviseurs non premiers avec le module. Ici, comme en Algèbre, $\frac{0}{0}$ apparaît comme un symbole d'indétermination, et $\frac{k}{0}$ comme un symbole d'impossibilité; si l'on considère même les deux termes par rapport à un diviseur quelconque du module donné pris comme nouveau module, $\frac{k}{0}$ reste un symbole d'impossibilité et $\frac{0}{0}$ devient un symbole d'indétermination relative. Cette indétermination n'est absolue que si les deux termes sont rapportés au module m; le quotient peut être, dans ce cas, l'un quelconque des chiffres $0, 1, 2, \ldots, m-1$.

Les Tables de division jouissent de propriétés intéressantes qui en facilitent la construction. On peut les regarder comme Tables de multiplication, en prenant un facteur dans la colonne d et suivant la ligne correspondante jusqu'à ce qu'on trouve l'autre facteur; le produit se lira alors sur la ligne D en tête de la colonne correspondante. Si nous prenons une ligne d'argument α, lu dans la colonne d et si nous marchons régulièrement sur cette ligne d'un pas α, nous atteindrons les cases successives ayant pour numéros 1α, 2α, 3α, ...; or ce sont justement les chiffres de la ligne D; de là, un moyen simple de construire la Table ligne par ligne. Remarquons en outre qu'une case ayant pour coordonnées $x = k\alpha$ et $y = \alpha$ devra contenir le chiffre k; donc la case de coordonnées $\lambda k\alpha$ et $\lambda\alpha$ contiendra le même chiffre, qui se trouvera dans toutes les cases d'une ligne partant de l'origine et définie par $kx + 1y$. En particulier, la diagonale partant de l'origine contient le chiffre 1 dans toutes ses cases. Cette remarque permet de construire mécaniquement la Table sans aucun calcul; elle explique aussi la différence capitale entre le cas d'un module premier et celui d'un module composé, les lignes arithmétiques dont nous venons de parler n'ayant aucune case commune dans le premier cas, et en ayant dans le second.

Un autre mode de construction pourrait s'obtenir par une méthode de superposition d'abaques (*Esp. ar.*, p. 45). Si le module m est le produit pq de deux facteurs premiers entre eux, supposons qu'on ait construit séparément la Table de division (P) de module p, et celle (Q) de module q, puis qu'on ait formé une figure en assemblant q^2 Tables (P) en un carré dont le côté sera m; et aussi une figure de p^2 Tables (Q) en un carré égal; ces deux carrés étant superposés, on considère une case quelconque résultant de la superposition de deux cases composantes; si l'une de ces cases composantes est blanche, la case résultante le sera aussi; si l'une contient un chiffre a (inférieur à p) dans la première figure, et l'autre un chiffre b (inférieur à q) dans la seconde, on inscrira le chiffre c (module m) qui s'écrit à la fois a dans le cas du module p et b dans celui du module q. Les deux Tableaux qui composent la figure 8 *bis* achèveront d'éclaircir tout ceci, en les examinant avec un peu d'attention. Ils représentent la Table de division de module 12 en considérant respectivement les diviseurs 3 et 4 :

Fig. 8 *bis*.

d

D		0	1	2	3	4	5	6	7	8	9	10	11
		0	1	2	0	1	2	0	1	2	0	1	2
0	0	0 1, 2			0 1, 2			0 1, 2			0 1, 2		
1	1	0	1	2	0	1	2	0	1	2	0	1	2
2	2	0	2	1	0	2	1	0	2	1	0	2	1
3	0	0 1, 2			0 1, 2			0 1, 2			0 1, 2		
4	1	0	1	2	0	1	2	0	1	2	0	1	2
5	2	0	2	1	0	2	1	0	2	1	0	2	1
6	0	0 1, 2			0 1, 2			0 1, 2			0 1, 2		
7	1	0	1	2	0	1	2	0	1	2	0	1	2
8	2	0	2	1	0	2	1	0	2	1	0	2	1
9	0	0 1, 2			0 1, 2			0 1, 2			0 1, 2		
10	1	0	1	2	0	1	2	0	1	2	0	1	2
11	2	0	2	1	0	2	1	0	2	1	0	2	1

Fig. 8 *bis*.

d

D

		0	1	2	3	4	5	6	7	8	9	10	11
		0	1	2	3	0	1	2	3	0	1	2	3
0	0	0, 1 2, 3				0, 1 2, 3				0, 1 2, 3			
1	1	0	1	2	3	0	1	2	3	0	1	2	3
2	2	0 2		1 3		0 2		1 3		0 2		1 3	
3	3	0	3	2	1	0	3	2	1	0	3	2	1
4	0	0, 1 2, 3				0, 1 2. 3				0, 1 2, 3			
5	1	0	1	2	3	0	1	2	3	0	1	2	3
6	2	0 2		1 3		0 2		1 3		0 2		1 3	
7	3	0	3	2	1	0	3	2	1	0	3	2	1
8	0	0, 1 2, 3				0, 1 2, 3				0, 1 2, 3			
9	1	0	1	2	3	0	1	2	3	0	1	2	3
10	2	0 2		1 3		0 2		1 3		0 2		1 3	
11	3	0	3	2	1	0	3	2	1	0	3	2	1

Fig. 8 *bis*.

d

D		0	1	2	3	4	5	6	7	8	9	10	11
		0	1	2	0	1	2	0	1	2	0	1	2
0	0	0 1, 2			0 1, 2			0 1, 2			0 1, 2		
1	1	0	1	2	0	1	2	0	1	2	0	1	2
2	2	0	2	1	0	2	1	0	2	1	0	2	1
3	0	0 1, 2			0 1, 2			0 1, 2			0 1, 2		
4	1	0	1	2	0	1	2	0	1	2	0	1	2
5	2	0	2	1	0	2	1	0	2	1	0	2	1
6	0	0 1, 2			0 1, 2			0 1, 2			0 1, 2		
7	1	0	1	2	0	1	2	0	1	2	0	1	2
8	2	0	2	1	0	2	1	0	2	1	0	2	1
9	0	0 1, 2			0 1, 2			0 1, 2			0 1, 2		
10	1	0	1	2	0	1	2	0	1	2	0	1	2
11	2	0	2	1	0	2	1	0	2	1	0	2	1

Fig. 8 *bis*.

d

D

		0	1	2	3	4	5	6	7	8	9	10	11
		0	1	2	3	0	1	2	3	0	1	2	3
0	0	0, 1 2, 3				0, 1 2, 3				0, 1 2, 3			
1	1	0	1	2	3	0	1	2	3	0	1	2	3
2	2	0 2		1 3		0 2		1 3		0 2		1 3	
3	3	0	3	2	1	0	3	2	1	0	3	2	1
4	0	0, 1 2, 3				0, 1 2, 3				0, 1 2, 3			
5	1	0	1	2	3	0	1	2	3	0	1	2	3
6	2	0 2		1 3		0 2		1 3		0 2		1 3	
7	3	0	3	2	1	0	3	2	1	0	3	2	1
8	0	0, 1 2, 3				0, 1 2, 3				0, 1 2, 3			
9	1	0	1	2	3	0	1	2	3	0	1	2	3
10	2	0 2		1 3		0 2		1 3		0 2		1 3	
11	3	0	3	2	1	0	3	2	1	0	3	2	1

Nous nous contentons d'indiquer ici cette méthode, qui peut sembler pénible, mais qui se simplifie et se généralise par l'emploi de Tables que nous étudierons un peu plus loin. Ajoutons, pour éviter toute équivoque, que si les cases composantes contiennent plusieurs chiffres a, a', a'', ... et b, b', b'', ..., on devra former toutes les associations d'un a quelconque avec un b quelconque, et procéder comme nous venons de le dire. Nous engageons le lecteur à étudier à ce point de vue la figure 6, module 15, en construisant les Tables de modules 3 et 5 et en effectuant la superposition des abaques comme nous venons de l'indiquer; il reconnaîtra, par exemple, que la case correspondant à $D = 1$, $d = 2$ s'obtient par la superposition des deux nombres 2 (abaque de module 3) et 3 (abaque de module 5); le chiffre à y inscrire est donc 8, puisque $8 \equiv 2 \pmod 3$ et $8 \equiv 3 \pmod 5$. Dans la figure 6, on lit effectivement $\bar{7}$, qui équivaut à 8.

10. Il résulte de ce qui précède que la division de deux chiffres pour un module premier est uniforme si le diviseur est différent de zéro, multiforme lorsque le dividende et le diviseur sont nuls, et impossible lorsque d est nul et que D ne l'est pas. Si le module est composé, il y a des divisions impossibles et des divisions multiformes dans toutes les lignes correspondant à un diviseur d non premier avec le module. Il est d'ailleurs presque évident que le nombre total des divisions uniformes est $m\,\varphi(m)$ puisque les quotients remplissent $\varphi(m)$ lignes et sont au nombre de m dans chacune.

Cette impossibilité de la division dans certains cas peut s'exprimer en disant que le quotient est imaginaire. Nous pourrons alors regarder, par exemple, le symbole $\left(\frac{9}{4}\right)$ ou $\left(\frac{\bar{3}}{4}\right)$ comme exprimant une certaine imaginaire arithmétique, n'ayant d'ailleurs que le nom de commun avec les imaginaires de l'Algèbre.

Une propriété assez intéressante au point de vue des applications est la suivante : si, ayant pris un diviseur α dans la colonne d on suit la ligne de α jusqu'à ce qu'on trouve un certain chiffre β, puis si l'on suit la ligne β jusqu'à ce qu'on trouve α, le β de la ligne α et l'α de la ligne β seront dans une même colonne, ce qui est évident puisque les produits $\alpha\beta$ et $\beta\alpha$ sont identiques. La véri-

fication se fera immédiatement sur les diverses figures données, que le module soit premier ou composé.

Tables de division réduites.

11. Pour le cas d'un module m composé, il y a souvent grand avantage à ne considérer dans la Table de division que les éléments qui correspondent à des chiffres de la ligne D et de la colonne d premiers avec m. Pour l'exemple $m = 12$, nous avons ainsi la Table réduite que voici :

D \ d				
0	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Dans cette Table, toutes les cases sont remplies, et les seuls éléments qui y figurent sont les chiffres premiers au module 12. Tous les chiffres d'une ligne sont différents, car les produits d'un chiffre par deux autres chiffres identiques sont identiques. Les chiffres d'une colonne sont aussi tous différents; en effet, si le même chiffre β se rencontrait deux fois dans une même colonne correspondant à l'argument a de la ligne D et aux arguments α et α' de la colonne d, nous aurions

$$a = \beta\alpha = \beta\alpha';$$

d'où

$$\beta(\alpha - \alpha') = 0;$$

et c'est impossible, puisque β est premier avec m et que $\alpha - \alpha'$ est inférieur à m. Cette circonstance se produit au contraire dans la

Table complète; par exemple

$$5.8 = 8.8 = 4$$

parce que $(8 - 5)8$ est un multiple de 12, 8 n'étant pas premier avec 12.

Remarquons encore : que la première ligne et la première colonne de la Table réduite présentent les chiffres premiers avec m dans l'ordre de leurs grandeurs croissantes; que la dernière ligne et la dernière colonne les présentent dans l'ordre inverse; que l'une des diagonales contient le chiffre 1 seulement, et l'autre le chiffre 11 ou $m - 1$. Enfin, la figure est symétrique par rapport à ses deux diagonales.

Mais ces diverses observations doivent être regardées de très près et ne constituent pas toutes des propriétés générales. Reprenons-les une à une.

La première ligne présente les chiffres dans leur ordre croissant, c'est-à-dire reproduit la ligne D. — C'est toujours vrai, car

$$1.\beta = \beta.$$

La première colonne présente les mêmes chiffres. — Ceci veut dire que $\alpha^2 = 1$, quel que soit α, premier avec m. Cela a lieu pour $m = 12$, mais non pas en général. Mais ce qu'on peut affirmer, c'est que la première et la dernière colonne présentent les mêmes éléments dans l'ordre inverse, c'est-à-dire que chaque ligne a pour extrémités deux chiffres dont la somme est m. En effet, si $\alpha a = 1$, il s'ensuit

$$\alpha(m - a) = m - 1;$$

plus généralement, la somme des deux chiffres de chaque ligne, symétriques par rapport à son milieu, est égale à m, parce que de $\alpha a = \beta$, on déduit

$$\alpha(m - a) = m - \beta.$$

La dernière ligne présente les chiffres dans l'ordre inverse.

— C'est toujours vrai, car

$$(m-1)\beta = 1(m-\beta).$$

Plus généralement, dans chaque colonne, les chiffres symétriques par rapport au milieu ont pour somme m, car

$$\alpha\beta = (m-\alpha)(m-\beta).$$

Les deux diagonales contiennent toujours, l'une 1, *l'autre* $m-1$. — C'est toujours exact, et cela résulte de la construction même. On peut ajouter, propriété générale aussi, que *la figure est toujours symétrique par rapport à son centre;* mais elle ne l'est pas toujours par rapport aux diagonales. Cette symétrie par rapport au centre résulte de la relation

$$a(m-\alpha) = (m-a)\alpha,$$

qu'on peut encore écrire

$$\frac{m-a}{m-\alpha} = \frac{a}{\alpha}.$$

La symétrie par rapport aux diagonales répondrait à la relation

$$\frac{a}{\alpha} = \frac{\alpha}{a} \quad \text{ou} \quad a^2-\alpha^2=0 \quad \text{ou} \quad (a+\alpha)(a-\alpha)=0,$$

qui est bien vraie pour $m=12$, mais non pas toujours. Pour rendre plus claires encore ces diverses remarques, nous donnons ici la Table réduite de division congruente pour le module 10 :

D \ d	0	1	3	7	9
	1	1	3	7	9
	3	7	1	9	3
	7	3	9	1	7
	9	9	7	3	1

Application; théorème de Fermat.

12. Puisque dans chaque colonne de la Table de division réduite nous avons tous les chiffres α, β, γ, ... premiers au module, et au nombre de $\varphi(m)$, en les associant aux chiffres correspondants de la colonne d nous aurons toujours le même chiffre λ de la ligne D pour produit. Donc, en appelant α', β', γ', ... dans leur ordre, ces chiffres de la colonne d, qui ne sont autres que α, β, γ, ..., nous avons

$$\alpha\alpha' = \beta\beta' = \gamma\gamma' = \ldots = \lambda.$$

De là

$$\alpha\beta\gamma\ldots\alpha'\beta'\gamma'\ldots = (\alpha\beta\gamma\ldots)^2 = \lambda^{\varphi(m)}.$$

Mais c'est vrai pour toute colonne, et par conséquent λ est arbitraire, parmi les chiffres α, β, ... au nombre desquels figure 1. Donc enfin,

$$\alpha^{\varphi(m)} = \beta^{\varphi(m)} = \ldots = 1^{\varphi(m)} = 1.$$

C'est le théorème de Fermat sous sa forme généralisée, pour un nombre composé. Notre démonstration établit en même temps que

$$(\alpha\beta\gamma\ldots)^2 = 1.$$

Dans le cas d'un nombre premier, on aura

$$\varphi(m) = m - 1.$$

Tables de numération.

13. Nous avons vu plus haut comment, pour former une Table de division par la méthode des abaques, on était ramené au problème suivant : m étant un module composé, $m_1 . m_2$ par exemple, et en supposant m_1, m_2 premiers entre eux, un chiffre μ est égal à μ_1 par rapport au module m_1 et à μ_2 par rapport à m_2. Trouver ce chiffre μ. La question est d'une grosse importance dans la théorie des équa-

tions arithmétiques, car elle touche de très près au principe que voici :

Lorsqu'on a A = 0 *par rapport à un module composé*

$$m = 2^{\nu} a^{\alpha} b^{\beta} c^{\gamma} \ldots,$$

on a simultanément A = 0 *pour chacun des modules* 2^{ν}, a^{α}, b^{β}, c^{γ}, ..., *et réciproquement.*

C'est à la solution du problème précédent que peuvent utilement servir les Tables de numération qui dispensent de tout calcul, et dont nous donnons un spécimen (*fig.* 9) pour le module 65 = 13.5. Pour construire cette Table, nous écrivons d'abord à la suite les uns des autres tous les chiffres du module 13.5 en commençant par 1 et en finissant par 0, ou 65. Au-dessous, en partant de la même verticale, écrivons de même la suite des chiffres de module 13 et répétons-la jusqu'à la verticale du 0 de la première ligne. Enfin, faisons-en autant pour les chiffres du module 5.

Table de numération de module 13.5.

Fig. 9.

13.5	1	2	3	4	5	6	7	8	9	10	11	12	13
13	1	2	3	4	5	6	7	8	9	10	11	12	0
5	1	2	3	4	0	1	2	3	4	0	1	2	3
13.5	14	15	16	17	18	19	20	21	22	23	24	25	26
13	1	2	3	4	5	6	7	8	9	10	11	12	0
5	4	0	1	2	3	4	0	1	2	3	4	0	1
13.5	27	28	29	30	31	32	33	34	35	36	37	38	39
13	1	2	3	4	5	6	7	8	9	10	11	12	0
5	2	3	4	0	1	2	3	4	0	1	2	3	4
13.5	40	41	42	43	44	45	46	47	48	49	50	51	52
13	1	2	3	4	5	6	7	8	9	10	11	12	0
5	0	1	2	3	4	0	1	2	3	4	0	1	2
13.5	53	54	55	56	57	58	59	60	61	62	63	64	65
13	1	2	3	4	5	6	7	8	9	10	11	12	0
5	3	4	0	1	2	3	4	0	1	2	3	4	0

En vertu de la théorie des marches sur les espaces linéaires, les nombres 13, 5 étant premiers entre eux, les diverses verticales contiendront sans répétition toutes les combinaisons de chiffres possibles, et réciproquement, il sera facile de retrouver une combinaison donnée à l'avance, et de lire, au-dessus, le chiffre correspondant par rapport au module 65. Il nous semble toutefois intéressant, pour une commodité encore plus grande, d'adjoindre (*fig.* 10) la Table qui donne les nombres connaissant les combinaisons.

Table de numération inverse de module 13.5.

Fig. 10.

5

13	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	40	15	55	30	5	45	20	60	35	10	50	25
1	26	1	41	16	56	31	6	46	21	61	36	11	51
2	52	27	2	42	17	57	32	7	47	22	62	37	12
3	13	53	28	3	43	18	58	33	8	48	23	63	38
4	39	14	54	29	4	44	19	59	34	9	49	24	64

L'extension à trois facteurs ou plus se comprend d'elle-même et conduirait à la construction de Tables de numération analogues.

14. La Table de numération inverse (*fig.* 10) mérite que nous nous y arrêtions quelques instants, car elle nous présente un exemple intéressant de ce que nous pourrions appeler *un espace bi-modulaire*. Elle se construira mécaniquement en formant la ligne $1x + 1y$, et en prenant 13 pour module des x et 5 pour module des y. Cette ligne comprendra toutes les cases du Tableau rectangulaire, et il en sera ainsi chaque fois que les deux modules p, q seront premiers entre eux. La dernière case, en bas à droite, sera numérotée $pq - 1$.

Il est d'ailleurs à remarquer que toute ligne arithmétique, dans un pareil espace, couvrirait également la totalité des cases; mais au point de vue de la Table de numération, la ligne $1x + 1y$ est la seule qui nous importe.

L'extension à des facteurs en nombre supérieur à 2, au moyen d'espaces analogues multi-modulaires, est toute naturelle. Pour plus de précision, considérons les trois facteurs 3, 7, 11; nous aurons alors un espace tri-modulaire (à trois dimensions) représenté par les trois Tableaux de la figure 11.

Fig. 11.

0

	0	1	2	3	4	5	6	7	8	9	10
0	0	210	189	168	147	126	105	84	63	42	21
1	99	78	57	36	15	225	204	183	162	141	120
2	198	177	156	135	114	93	72	51	30	9	219
3	66	45	24	3	213	192	171	150	129	108	87
4	165	144	123	102	81	60	39	18	228	207	186
5	33	12	222	201	180	159	138	117	96	75	54
6	132	111	90	69	48	27	6	216	195	174	153

1

	0	1	2	3	4	5	6	7	8	9	10
0	154	133	112	91	70	49	28	7	217	196	175
1	22	1	211	190	169	148	127	106	85	64	43
2	121	100	79	58	37	16	226	205	184	163	142
3	220	199	178	157	136	115	94	73	52	31	10
4	88	67	46	25	4	214	193	172	151	130	109
5	187	166	145	124	103	82	61	40	19	229	208
6	55	34	13	223	202	181	160	139	118	97	76

2

	0	1	2	3	4	5	6	7	8	9	10
0	77	56	35	14	224	203	182	161	140	119	98
1	176	155	134	113	92	71	50	29	8	218	197
2	44	23	2	212	191	170	149	128	107	86	65
3	143	122	101	80	59	38	17	227	206	185	164
4	11	221	200	179	158	137	116	95	74	53	32
5	110	89	68	47	26	5	215	194	173	152	131
6	209	188	167	146	125	104	83	62	41	20	230

Cette figure 11 va nous permettre de préciser quelques propriétés générales de ces espaces multi-modulaires et d'en tirer certaines conséquences. Nous désignerons par $M = m_1 m_2 \ldots$ le module, par m_1, m_2, ..., ses facteurs premiers entre eux (3, 7, 11, sur la figure).

Si, partant de la case origine, on marche simultanément du pas 1 suivant les trois directions coordonnées, on parcourra une certaine route dont la longueur sera égale au nombre des pas. Plaçant, dans chaque case rencontrée, un nombre égal au nombre des pas effectués, chacun de ces nombres sera un chiffre de module M. La projection de cette case, sur chacun des axes coordonnés, nous donnera le nombre correspondant écrit suivant chacun des modules m_1, m_2, ...

A mesure que le mobile supposé poursuit sa marche, suivons celle de sa projection sur l'une des directions coordonnées x_1, par exemple sur la direction horizontale de la figure, correspondant à 11. La route suivie ne pourra rencontrer cet axe coordonné avant d'avoir effectué 3.7 pas $\left(\text{en général } \frac{M}{m_1}\right)$ et à cet instant elle le coupera forcément; $\frac{M}{m_1}$ (ici 21) sera écrit suivant le module m_1, le numéro de la case où aura lieu l'intersection; ici ce sera $10 = 21$, module 11. Tous les 21 pas il y aura une nouvelle intersection, et les cases rencontrées seront les multiples successifs de 10. Quand l'intersection se fera à la case 1, le nombre de pas parcourus sera donc $\frac{1}{10} \times 21$, la fraction $\frac{1}{10}$ représentant, module 11, le quotient de 1 par 10; c'est ici 10, et 210 sera le nombre à inscrire dans la case. Naturellement, chaque case devra contenir un nombre égal au produit de 210 pas le rang de la case. En général, si k_1 est ce rang, nous aurons

$$\frac{M}{m_1} k_1 \left(\frac{m_1}{M}\right).$$

On peut en dire autant pour chacune des coordonnées, et il en résulte la construction des lignes de bordure suivant chaque direction. Une case de l'intérieur de l'espace contenant un nombre qui n'est autre que la somme de ses projections sur chacune des lignes de bordure, nous avons donc pour ce nombre la formule intéres-

sante

$$K = \sum \frac{M}{m_i} k_i \left(\frac{m_i}{M}\right),$$

le signe $\sum$ s'étendant à tous les facteurs m_i et le symbole entre parenthèses étant calculé par rapport au facteur m_i.

De cette formule nous allons donner un peu plus loin une démonstration purement analytique. Nous laissons au lecteur le soin d'en faire application aux exemples qu'il pourra emprunter aux figures 10 et 11.

Dans l'espace de module 3.7.11, on peut étudier la formation des plans qu'il contient. Si, par exemple, dans le premier plan de modules (7, 11) on suit la diagonale partant de la case origine, tous les trois pas elle rencontrera les cases numérotées 3, 6, 9, ... et l'on pourra, mécaniquement pour ainsi dire, former ainsi tout le Tableau. De même pour 1, 4, 7, ... dans le deuxième Tableau, et pour 2, 5, 8, ... dans le troisième. Ces remarques permettent donc de former à vue, sans calcul, les espaces multi-modulaires dont il s'agit, et d'y constater les propriétés intéressantes qui leur appartiennent et qui pourraient être utilisées dans beaucoup d'autres questions arithmétiques.

Analytiquement, le problème que nous venons de résoudre par les Tables de numération inverses est le suivant. On a

$$M = m_1 m_2 \ldots$$

(m_1, m_2, ... étant premiers entre eux) et

$$K = m_1 x_1 + k_1 = m_2 x_2 + k_2 = \ldots;$$

déterminer ce nombre K, par rapport au module M.

Pour simplifier, supposons trois facteurs m_1, m_2, m_3 seulement, ce qui ne particularise pas le raisonnement, et écrivons

$$\frac{m_1}{M} = \mu_1,$$

c'est-à-dire

$$\frac{1}{m_2 m_3} = \mu_1 \qquad (\text{mod}\, m_1).$$

Nous avons

$$m_2 m_3 K = M x_1 + m_2 m_3 k_1,$$

d'où

$$m_2 m_3 \mu_1 K = M \mu_1 x_1 + m_2 m_3 k_1 \mu_1,$$

et deux autres relations analogues. Par addition, il vient

$$(m_2 m_3 \mu_1 + m_3 m_1 \mu_2 + m_1 m_2 \mu_3) K = \sum \frac{M}{m_i} k_i \left(\frac{m_i}{M}\right) \quad (\text{mod}\, M);$$

or, puisque $m_2 m_3 \mu_1$ est un multiple de m_1, plus 1, le coefficient de K est lui-même un multiple de m_1, plus 1; de même, c'est un multiple de m_2, plus 1, et de m_3, plus 1; c'est donc un multiple de M, plus 1, ce qui démontre la formule.

Remarque. — En posant comme plus haut $\left(\frac{m_i}{M}\right) = \mu_i$, on voit que $\sum \frac{\mu_i}{m_i} - \frac{1}{M}$ est toujours un entier X; le coefficient de K dans la relation précédente est alors $MX + 1$.

CHAPITRE II.

PUISSANCES ET RACINES DES ENTIERS.

Puissances et indices.

15. Si nous considérons les puissances successives d'un nombre entier a,

$$a^1, \quad a^2, \quad a^3, \quad \ldots, \quad a^p, \quad \ldots,$$

écrites suivant un espace linéaire indéfini, et si nous écrivons sur une ligne correspondante les exposants successifs,

$$1, \quad 2, \quad 3, \quad \ldots, \quad p, \quad \ldots,$$

le rapprochement de ces deux espaces forme en réalité une Table de logarithmes, dans laquelle les termes de la première ligne sont les *nombres*, et ceux de la seconde ligne les *logarithmes;* la *base* n'est autre que le nombre lui-même. Mais tandis que dans la théorie ordinaire, arithmétique ou algébrique, la notion de la continuité s'impose, aussi bien pour les nombres que pour les logarithmes, nous avons ici affaire à des fonctions numériques essentiellement discontinues, tous les termes devant être des nombres entiers. Malgré cela, on peut remarquer que la propriété fondamentale des logarithmes subsiste intégralement, c'est-à-dire que le logarithme d'un produit est égal à la somme des logarithmes des facteurs.

Cette notion générale étant établie, remarquons que nous pouvons congruer les nombres a^1, a^2, ... par rapport à un module m, que tout d'abord nous supposerons premier. Dès lors, chacun des termes deviendra un chiffre de m, et l'espace indéfini se transformera en un espace congruent. Les égalités se transformeront en

congruences, et, en particulier, en vertu du théorème de Fermat, lorsque nous serons parvenu au terme a^{m-1}, nous pourrons le remplacer par 1; à partir de là, nous retrouverons tous les mêmes termes périodiquement. Examinons maintenant ce qui se passe pour les termes de la seconde ligne, que nous pouvons appeler *logarithmes modulaires,* selon la dénomination de Gauss; au nombre a^{m-1} correspond le logarithme $m-1$; au nombre suivant a^m correspondrait m; mais $a^m = a$ suivant le module m, et a possède pour logarithme 1. Pour que la correspondance existe régulièrement entre les deux suites, il faut donc que nous écrivions les logarithmes

$$1,\quad 2,\quad 3,\quad \ldots,\quad m-1,\quad 1,\quad 2,\quad 3,\quad \ldots,$$

c'est-à-dire que, tandis que les nombres sont congrués suivant le module m, les logarithmes doivent l'être suivant le module $m-1$. Cette remarque générale est d'une haute importance, et l'on reconnaît immédiatement qu'on peut l'étendre à un module non premier, en remplaçant $m-1$ par $\varphi(m)$.

Il semble y avoir du reste avantage à employer le mot *indice* (qui a cours lui aussi en théorie des nombres) de préférence à celui de logarithme, et c'est ce que nous ferons désormais.

Cycles.

16. Dans ce qui précède, nous n'avons rien supposé relativement à la *base* a du système qui donne naissance à la Table des indices. Il y a cependant une distinction capitale à établir, distinction dont quelques simples exemples vont nous permettre de nous rendre compte. Ici encore, nous nous bornerons au cas d'un module premier, 13 par exemple; on peut toujours admettre que a est un chiffre de 13, car, si

$$a = m13 + \alpha,$$

on remplacera a par α et l'on aura identiquement les mêmes résultats.

Soit donc $a = 3$; en élevant 3 à ses puissances successives, et



en congruant par 13, nous obtenons

$$3 \quad 9 \quad 1 \quad 3 \quad 9 \quad 1 \quad \ldots$$

Si bien que les indices, si nous les écrivions de 1 à 12, se trouveraient ne plus correspondre uniformément aux nombres, puisque à un même nombre répondraient plusieurs indices différents.

Au contraire, prenons $a = 4$; la suite des nombres est

$$4 \quad 3 \quad 12 \quad 9 \quad 10 \quad 1 \quad 4 \quad 3 \quad \ldots$$

La période, qui tout à l'heure était de trois termes, en comprend maintenant six.

Enfin, prenons $a = 7$; nous avons

$$7 \quad 10 \quad 5 \quad 9 \quad 11 \quad 12 \quad 6 \quad 3 \quad 8 \quad 4 \quad 2 \quad 1 \quad 7 \quad \ldots$$

et ici le nombre des termes de la période est $m - 1$ ou 12.

Les divers résultats que nous venons de constater s'énoncent souvent en disant que, par rapport au module 13, le chiffre 3 appartient à l'exposant (ou à l'indice) 3, le chiffre 4 à l'indice 6, et le chiffre 7 à l'indice 12. Il nous semble préférable de dire simplement que les nombres des termes de leurs périodes sont 3, 6, 12.

Quand un chiffre a pour nombre des termes de sa période $m - 1$, on dit que c'est une *racine primitive* du module m. Par exemple, 7 est une racine primitive de 13.

Les périodes que nous venons d'écrire dans les exemples précédents peuvent s'obtenir d'une façon systématique par un procédé graphique des plus simples, en nous servant de la Table de multiplication. Il suffit pour cela d'accoler, à la ligne du cadre, celle qui répond au multiplicateur a écrit dans la première colonne.

Ainsi, pour reprendre les trois exemples précédents, construisons les éléments que nous venons de dire, et nous aurons :

($a = 3$)	0	1	2	3	4	5	6	7	8	9	10	11	12
	0	3	6	9	12	2	5	8	11	1	4	7	10
($a = 4$)	0	1	2	3	4	5	6	7	8	9	10	11	12
	0	4	8	12	3	7	11	2	6	10	1	5	9
($a = 7$)	0	1	2	3	4	5	6	7	8	9	10	11	12
	0	7	1	8	2	9	3	10	4	11	5	12	6

Ceci fait, prenons, dans l'une quelconque de ces trois figures, le nombre a dans la première ligne, et lisons le nombre a_1 de la seconde ligne qui lui correspond; puis prenons a_1 dans la première ligne, et le nombre a_2 qui lui correspond dans la seconde; et ainsi de suite; nous aurons respectivement

(3 9 1) 3 9 1 ...
(4 3 12 9 10 1) 4 3 12 ...
(7 10 5 9 11 12 6 3 8 4 2 1) 7 10 5 ...

L'ensemble des termes périodiques compris dans les parenthèses forme un *cycle*. On voit combien ce mécanisme des cycles, pratiqué sur la Table de multiplication, est de nature à faciliter la construction des puissances, sans aucun calcul, et comment cette théorie des cycles se lie étroitement à celle des indices ou logarithmes modulaires.

Génération graphique des puissances.

17. Élever un nombre à ses puissances successives, c'est marcher sur l'espace arithmétique

0 1 2 3 ...

de la façon suivante. A partir de l'origine, on fait 1 pas a; ou, ce qui revient au même, a pas de 1; puis, d'une marche régulière, on fait a pas de a, ce qui donne un certain élément, comme extrémité de la route suivie. Prenant la distance de l'origine à cet élément comme pas, on fait encore a pas; et ainsi de suite, en prenant chaque fois comme longueur du pas la route totale que l'on a faite. Le nombre total des opérations donne le degré de la puissance.

En congruant, suivant un module m, on voit à quelles opérations graphiques se réduit la recherche des chiffres congruents aux puissances successives, et comment cette opération se rattache à la formation des cycles, ainsi que nous l'avons indiqué précédemment. On substitue ainsi une opération mécanique très simple à un calcul parfois long et pénible.



Table des puissances.

18. Nous considérerons exclusivement dans ce paragraphe le cas d'un module premier. Prenons par exemple 13. Si nous formons, par le procédé que nous venons de dire, la suite des chiffres congruents aux puissances successives de 1, puis de 2, de 3, ..., en accolant ligne par ligne tous ces résultats, nous aurons (*fig.* 12) la Table des puissances congruentes pour le module 13. La ligne du cadre I est celle des indices ou exposants. La colonne du cadre N est celle des nombres (ici réduits à des chiffres du module). Le corps de la Table donne donc toutes les puissances de tous les nombres.

Table des puissances (mod 13).

Fig. 12.

N \ I	1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	3	6	12	11	9	5	10	7	1
3	3	9	1	3	9	1	3	9	1	3	9	1
4	4	3	12	9	10	1	4	3	12	9	10	1
5	5	12	8	1	5	12	8	1	5	12	8	1
6	6	10	8	9	2	12	7	3	5	4	11	1
7	7	10	5	9	11	12	6	3	8	4	2	1
8	8	12	5	1	8	12	5	1	8	12	5	1
9	9	3	1	9	3	1	9	3	1	9	3	1
10	10	9	12	3	4	1	10	9	12	3	4	1
11	11	4	5	3	7	12	2	9	8	10	6	1
12	12	1	12	1	12	1	12	1	12	1	12	1

Sur cette figure, plusieurs constatations sont immédiates. D'abord la première ligne ne comprend que des 1, puisque $1^\alpha = 1$ quel que soit α. La dernière colonne, répondant à l'indice 12, ne comprend également que des 1, ce qui doit arriver en vertu du théorème de Fermat. Deux lignes symétriques par rapport au diamètre horizontal, par exemple celles qui répondent aux arguments 5 et 8 de la colonne N

$$\begin{array}{cccccccccccc} 5 & 12 & 8 & 1 & 5 & 12 & 8 & 1 & 5 & 12 & 8 & 1 \\ 8 & 12 & 5 & 1 & 8 & 12 & 5 & 1 & 8 & 12 & 5 & 1 \end{array}$$

sont telles que les termes d'indices pairs sont identiques, et que les termes d'indices impairs ont pour somme 13. En se servant des chiffres négatifs, on aurait

$$\begin{array}{cccccccccccc} 5 & \bar{1} & \bar{5} & 1 & 5 & \bar{1} & \bar{5} & 1 & 5 & \bar{1} & \bar{5} & 1 \\ \bar{5} & \bar{1} & 5 & 1 & \bar{5} & \bar{1} & 5 & 1 & \bar{5} & \bar{1} & 5 & 1 \end{array}$$

Cela résulte de ce que

$$a^n = (m - a)^n,$$

si n est pair, et

$$-(m - a)^n,$$

si n est impair.

Entre les différentes lignes, il y a des distinctions importantes à établir. Les unes comprennent tous les chiffres de 1 à 12 et forment une période de 12 termes; les autres forment bien une période de 12 termes, mais qui se subdivise en des périodes moindres. Autrement dit, on rencontre 1 avant la colonne d'indice 12, et l'indice qui correspond au premier 1 qu'on rencontre est, d'après ce que nous avons dit plus haut, l'exposant auquel appartient le nombre de la colonne N. Ainsi 2, 6, 7, 11 ont 12 pour nombre de termes de leur période, c'est-à-dire sont des racines primitives de 13; pour 4 et 10, ce nombre est 6; pour 5 et 8, 4; pour 3 et 9, 3; pour 12, 2; et pour 1, 1. Ces divers nombres sont des diviseurs de 12, ou $m - 1$; s'il en était autrement, si 5, par exemple, pouvait correspondre à a, on aurait

$$a^5 = 1;$$

il en serait de même pour a^n, n étant un multiple quelconque de 5;

or, comme en marchant sur l'espace

0 1 2 3 4 5 6 7 8 9 10 11 12

d'un pas régulier de 5, et en congruant par 12, on rencontre tous les chiffres de 12, il s'ensuit que l'on aurait 1 partout, ce qui ne peut arriver que pour le nombre 1. Si, au lieu de 5, nous avions pris 8, qui n'est pas premier avec 12, mais qui n'est pas non plus un diviseur de 12, il est clair que la marche de pas 8 donnerait en particulier le plus grand codiviseur de 8 et de 12, c'est-à-dire 4; donc 8 ne peut pas être le nombre des termes de la période d'un nombre quelconque, puisque ce codiviseur 4 est nécessairement plus petit.

Quand on prend une période quelconque,

5 12 8 1

par exemple, qui répond à 5, tous les chiffres 5, 12, 8, 1 appartiennent au même exposant, nombre des termes de la période, ou à un exposant moindre. Cela a lieu pour ceux (5, 8) dont les rangs, ou les indices, sont premiers avec 12; les deux autres appartiennent, au contraire, à des exposants moindres.

Table des racines.

19. De la Table des puissances, il est aisé de déduire une Table des racines (*fig.* 13) dont la construction s'explique d'elle-même, la ligne du cadre I représentant les indices des racines, et les chiffres de la colonne P, les puissances dont on demande d'extraire les racines. On pourrait même imaginer une troisième Table, celle des indices, en prenant p et n pour arguments, dans la relation $p = n^i$, mais nous croyons inutile ici de la construire.

Table des racines (mod 13).

Fig. 13.

P

	1	2	3	4	5	6	7	8	9	10	11	0
1	1	1 12	1 3 9	1 5 8 12	1	1 3 4 9 10 12	1	1 5 8 12	1 3 9	1 12	1	1 2 3 4 5 6 7 8 9 10 11 12
2	2				6		11				7	
3	3	4 9		2 3 10 11	9		3	4 6 7 9		3 10	9	
4	4	2 11			10		4			6 7	10	
5	5		7 8 11		5		8		2 5 6		8	
6	6				2		7				11	
7	7				11		6				2	
8	8		2 5 6		8		5		7 8 11		5	
9	9	3 10		4 6 7 9	3		9	2 3 10 11		4 9	3	
10	10	6 7			4		10			2 11	4	
11	11				7		2				6	
12	12	5 8	4 10 12		12	2 5 6 7 8 11	12		4 10 12	5 8	12	

Cette Table des racines, comparée à celle des puissances, présente des dissemblances analogues à celles qui existent entre la Table de division et celle de multiplication. Certaines cases restent blanches, tandis que d'autres renferment plusieurs chiffres. La première colonne est identique à celle du cadre. Tous les chiffres figurent dans chaque colonne, groupés par nombres égaux au plus grand codiviseur Δ, entre l'indice et $12 = m - 1$. Il y a par conséquent dans chaque colonne $\frac{m-1}{\Delta}$ cases remplies. Les colonnes d'indices 1, 5, 7, 11, premiers à 12, sont entièrement remplies et sont ici identiques à celles de la Table des puissances.

On remarquera qu'à la ligne I le dernier chiffre $m - 1 = 12$ a été remplacé par 0, les indices devant être congrués suivant $m - 1$.

Gaussien ; racines primitives.

20. Revenons à la Table des puissances (*fig.* 12) et prenons une ligne quelconque, celle d'argument 5, par exemple

$$5 \quad 12 \quad 8 \quad 1 \quad 5 \quad 12 \quad 8 \quad 1 \quad 5 \quad 12 \quad 8 \quad 1$$

La période est de 4 termes ; autrement dit, 5 appartient à l'exposant 4. Lucas a proposé de dire plus simplement que 4 est le *gaussien* de 5, et, dans ce qui suivra, nous nous servirons systématiquement de cette expression. Si dans la période

$$5 \quad 12 \quad 8 \quad 1$$

nous prenons les termes dont l'indice est premier avec 4, savoir 5 et 8, ils auront pour gaussien 4 ; les autres, 12 et 1, auront des gaussiens inférieurs, diviseurs de 4. En général, le nombre des chiffres ayant pour gaussien un diviseur d quelconque de $m - 1$ sera donc $\varphi(d)$. Or, comme tout chiffre a un certain gaussien, diviseur de $m - 1$, on aura

$$\varphi(1) + \varphi(2) + \ldots = \sum \varphi(d) = m - 1.$$

D'autre part, on sait que, pour tout nombre p, on a

$$\sum \varphi(\delta) = p,$$

δ représentant un diviseur quelconque de p, et la somme s'étendant à tous les diviseurs (y compris 1 et p). Il y a donc nécessairement des chiffres ayant pour gaussien un diviseur *quelconque* de $m-1$.

En particulier, ceci démontre qu'il y a des racines primitives, et qu'elles sont au nombre de $\varphi(m-1)$. On les a toutes, dès qu'on connaît la période de l'une quelconque d'entre elles, 7 par exemple :

7 10 5 9 11 12 6 3 8 4 2 1

Les chiffres 7, 11, 6, 2, dont les indices 1, 5, 7, 11 sont premiers à $m-1$, sont les racines primitives.

Dans la Table des racines, on remarque que les lignes correspondantes ne contiennent que quatre cases remplies [en général $\varphi(m-1)$], et que les chiffres qu'elles contiennent, un seul par case, sont précisément les racines primitives.

Si, à la période précédente d'une des racines primitives, nous adjoignons, au-dessus, la suite naturelle des indices, nous aurons une Table composée de deux lignes seulement

1	2	3	4	5	6	7	8	9	10	11	0
7	10	5	9	11	12	6	3	8	4	2	1

qu'on peut appeler *Table réduite* de puissances.

Ces Tables réduites présentent un intérêt considérable au point de vue des applications. Il faut remarquer que, pour les construire, on peut partir à volonté d'une racine primitive quelconque.

Modules composés.

21. Si l'on veut étudier le cas des modules composés, la formation des Tables de puissances n'offre pas théoriquement de plus grandes difficultés et elle peut notamment s'effectuer par la méthode des cycles qui est tout à fait générale. Mais les choses deviennent singulièrement complexes quand il s'agit d'aborder la question inverse, qui constitue le vrai problème à résoudre. C'est pourquoi il nous paraît nécessaire de compléter ce que nous venons de dire par une étude fondée sur une méthode nouvelle, que nous allons exposer.

Auparavant, rappelons quelques notions générales, absolument



essentielles. Tandis que l'on étudie les nombres eux-mêmes, par rapport au module m, les indices doivent être congrués par rapport à un module différent $\mathfrak{M}$. Si m est premier,

$$\mathfrak{M} = \varphi(m) = m - 1;$$

c'est l'indicateur (*Esp. ar.*, p. 79). Si $m = a^\alpha b^\beta \ldots$, $\mathfrak{M}$ est le plus petit comultiple de $\varphi(a^\alpha)$, $\varphi(b^\beta)$, ... ou l'indicateur réduit de m, souvent appelé $\psi(m)$. Plus loin, nous trouverons un module $\mathfrak{M}$ de la forme $m^n - 1$. Uniformément, nous adopterons l'expression *module des indices,* qui s'applique à tous les cas.

Quand on élève un nombre quelconque à ses puissances successives, la suite obtenue prend un caractère périodique; le nombre des termes de la période est le gaussien G; c'est un diviseur de $\mathfrak{M}$ et l'on peut écrire $CG = \mathfrak{M}$; C est le plus grand codiviseur avec $\mathfrak{M}$ de l'indice du nombre considéré, pris sur une suite complète, de $\mathfrak{M}$ termes.

Ces préliminaires établis, nous arrivons à l'exposé de la méthode, fondée sur les Tables de périodes, que nous allons présenter en l'appliquant au module $65 = 13.5$, pris pour exemple. Nous construisons d'abord les deux Tableaux suivants (*fig.* 14, 15) :

Table des périodes des chiffres ($m = 13$).

Fig. 14.

Indices			1	2	3	4	5	6	7	8	9	10	11	12
C			1	2	3	4	1	6	1	4	3	2	1	12
Puissances			2	4	8	3	6	12	11	9	5	10	7	1
a	4	12	2	.	.	.	6	.	11	.	.	.	7	.
b	2	6	.	4	.	.	.	.	.	.	.	10	.	.
c	2	4	.	.	8	.	.	.	.	.	5	.	.	.
d	2	3	.	.	.	3	.	.	.	9	.	.	.	.
e	1	2	.	.	.	.	.	12	.	.	.	.	.	.
f	1	1	.	.	.	.	.	.	.	.	.	.	.	1
	$\varphi(G)$	G												

Table des périodes des chiffres ($m = 5$).

Fig. 15.

Indices			1	2	3	4
C			1	2	1	4
Puissances			2	4	3	1
α	2	4	2	.	3	.
β	1	2	.	4	.	.
γ	1	1	.	.	.	1
	$\varphi(G)$	G				

La première ligne est la suite des indices, dont le dernier est leur module. La deuxième ligne donne C; la troisième, la suite des puissances d'un chiffre de période $\varphi(m)$.

La première colonne contient des lettres de référence représentant une ligne; la troisième, le gaussien G de chaque chiffre de la ligne; la deuxième, le nombre de termes de la ligne, nombre égal à $\varphi(G)$.

Tous les chiffres d'une ligne ont même gaussien.

Ainsi (2, 6, 7, 11), ayant $C = 1$, ont $2^2.3 = 12$ pour gaussien; (4, 10), ayant $C = 2$, leur gaussien est

$$2.3 = 6.$$

On peut, sur ce Tableau, vérifier la loi

$$C.G = \varphi(m).$$

Au moyen de ces deux figures, formons maintenant la suivante (*fig.* 16) :

Table d'association ($m = 13.5$).

Fig. 16.

			a	b	c	d	e	f	
			$2^2.3$	2.3	2^2	3	2	1	G_1
			4	2	2	2	1	1	$\varphi(G_1)$
α	2^2	2	A	A	B	A	B	B	
β	2	1	A	C	B	C	E	E	
γ	1	1	A	C	B	D	E	F	
	G_2	$\varphi(G_2)$							

La première ligne et la première colonne contiennent les lettres de référence des Tables de période des chiffres des modules com-

posants; les deuxième ligne et deuxième colonne les valeurs G décomposées en leurs facteurs premiers, les troisième ligne et troisième colonne les indicateurs des nombres G, c'est-à-dire $\varphi(G)$.

Dans l'intérieur du Tableau, les grandes lettres représentent les chiffres de module $\mathfrak{M}$ qui correspondent à l'association des chiffres compris dans les lignes du cadre représentées par une lettre de même nature dans les Tables de périodes des modules composants.

Leur situation sur la Table est déterminée par la condition que leur gaussien est le plus petit comultiple des gaussiens des modules composants.

Ainsi, les chiffres représentés par A ont pour gaussien $2^2.3$, plus petit comultiple des gaussiens $2^2.3$, représentés par a, et des gaussiens 2^2 représentés par α.

Le nombre des chiffres se rapportant à une situation de A est le produit des $\varphi(G)$ des lignes et colonnes du cadre.

Si, sur toute l'étendue du Tableau, on prend tous les chiffres A et si l'on fait la somme de ces produits, on a le nombre total des chiffres ayant (module $\mathfrak{M}$) un gaussien $2^2.3$.

Ce que je viens de dire pour la lettre A s'applique sans distinction à toutes les lettres du Tableau.

On voit donc ici que *la considération de plus petit comultiple n'est pas spéciale à l'indicateur réduit, nombre de chiffres correspondant à la plus grande période des puissances des chiffres de module* $\mathfrak{M}$, *mais qu'elle est absolument générale et s'applique à toutes les périodes sans distinction.*

Quant à la Table, elle est une application du principe des coordonnées aux espaces arithmétiques; toute case du Tableau est le plus petit comultiple des cases du cadre sur lesquelles elle se projette orthogonalement, et le nombre des chiffres de cette case est le produit des $\varphi(G)$ insérés dans les cases du cadre, comme dans la Table dite *de Pythagore*.

$$\begin{array}{llll}
A = 2(4+2+2) & +1.4+1.4 & = & 24\\
B = 2(2+1+1) & +1.2+1.2 & = & 12\\
C = 2(2+2) & +1.2 & = & 6\\
D = 1.2 & & = & 2\\
E = 1(1+1) & +1.1 & = & 3\\
F = 1.1 & & = & \underline{1}\\
 & & & 48
\end{array}$$

La Table ci-dessus donne le nombre de chiffres de chacune des catégories correspondant aux lettres A, B, C, D, E, F.

Au moyen de cette Table, il est facile de se rendre compte, non seulement de la forme de la Table des puissances de module 13.5, mais encore de son économie générale, considération que je regarde comme capitale.

Cette Table des puissances de module 13.5 (*fig.* 17) a pu être facilement construite, avec l'aide de la Table de numération que nous avons donnée plus haut. On remarquera que nous la bornons à six lignes, contenant tous les chiffres premiers au module, et dont chacune se termine par 1.

Table des puissances de module composé, $m = 13.5$.

TABLE ÉCRITE $m = 13.5$.

Fig. 17.

	1	2	3	4	5	6	7	8	9	10	11	12
1	2	4	8	16	32	64	63	61	57	49	33	1
2	37	4	18	16	7	64	28	61	47	49	58	1
3	3	9	27	16	48	14	42	61	53	29	22	1
4	62	9	38	16	17	14	23	61	12	29	43	1
5	11	56	31	16	46	51	41	61	21	36	6	1
6	54	56	34	16	19	51	24	61	44	36	59	1

TABLE ÉCRITE $m = 13$.

	1	2	3	4	5	6	7	8	9	10	11	12
1	2	4	8	3	6	12	11	9	5	10	7	1
2	11	4	5	3	7	12	2	9	8	10	6	1
3	3	9	1	3	9	1	3	9	1	3	9	1
4	10	9	12	3	4	1	10	9	12	3	4	1
5	11	4	5	3	7	12	2	9	8	10	6	1
6	2	4	8	3	6	12	11	9	5	10	7	1

Table des puissances de module composé, $m = 13.5$ (suite).

TABLE ÉCRITE $m = 5$.

Fig. 17.

	1	2	3	4	5	6	7	8	9	10	11	12
1	2	4	3	1	2	4	3	1	2	4	3	1
2	2	4	3	1	2	4	3	1	2	4	3	1
3	3	4	2	1	3	4	2	1	3	4	2	1
4	2	4	3	1	2	4	3	1	2	4	3	1
5	1	1	1	1	1	1	1	1	1	1	1	1
6	4	1	4	1	4	1	4	1	4	1	4	1

Jetant un coup d'œil sur cette Table, nous voyons que les chiffres de gaussien $2^2.3$ occupent les colonnes d'indice (1, 5, 7, 11) ayant avec $\psi(m)$ le plus grand codiviseur 1; ceux de gaussien 2.3 occupent les colonnes d'indice (2, 10) ayant avec $\psi(m)$ le plus grand codiviseur 2, et ainsi de suite.

Notons également que tout chiffre de gaussien 2.3 est un carré des chiffres de gaussien $2^2.3$; ou, si l'on veut, les seconds sont les racines carrées des premiers.

Les chiffres de gaussien 2.3 sont en nombre 6; comme il y a vingt-quatre chiffres de gaussien $2^2.3$, à chaque chiffre de gaussien 2.3 correspondent quatre chiffres $2^2.3$; *par suite toutes les lignes sont complètes.*

Quant au nombre de ces lignes, il sera de

$$\frac{24}{4} = \frac{12}{2} = 6.$$

Si l'on fait la somme des nombres de chiffres relatifs à chaque période, on voit qu'elle est égale à

$$48 = \varphi(m),$$

c'est-à-dire qu'elle comprend la totalité des chiffres premiers à m.

Je me contente de ces quelques observations; mais tout *visuel* peut, sur l'ensemble de ces Tableaux, lire une foule de propositions qui se passent de démonstration, ce qui est un des précieux avantages de la méthode graphique.

Pour ce qui va suivre, il est bon de se rendre compte de la situation des colonnes où doivent être inscrits les chiffres racines d'un chiffre de gaussien désigné.

Table de situation des racines, $m = 13.5$.

Fig. 18.

1	2	3	4	1	6	1	4	3	2	1	12	C
1	2	3	4	5	6	7	8	9	10	11	12	Indice
⊙	B	.	.	.	.	⊙	.	.	.	.	.	$\sqrt[2]{\ }$
.	.	.	.	⊙	.	.	.	.	B	⊙	.	
⊙	.	C	.	⊙	.	.	.	⊙	.	.	.	$\sqrt[3]{\ }$
.	.	⊙	.	.	.	⊙	.	C	.	⊙	.	
⊙	.	.	D	.	.	⊙	.	.	⊙	.	.	$\sqrt[4]{\ }$
.	⊙	.	.	⊙	.	.	D	.	.	⊙	.	
⊙	.	⊙	.	⊙	E	⊙	.	⊙	.	⊙	.	$\sqrt[6]{\ }$
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	F	$\sqrt[12]{\ }$

Dans le Tableau (*fig.* 18) la deuxième ligne du cadre est l'indice du chiffre sur la Table de module m; la première contient le plus grand codiviseur entre $\psi(m)$ et l'indice situé au-dessous. Dans l'intérieur du Tableau, les points entourés d'un rond marquent le

rang de la colonne où sont situées les racines des chiffres symbolisés par les diverses lettres.

Au moyen des éléments qui précèdent, voyons maintenant comment a pu être construite la Table de la figure 17.

Prenons au hasard une des associations représentées par A, soit 2, module 13, et 2, module 5; faisons la période de 2, module 13, nous avons la première ligne de la Table des puissances, écrite module 13; faisons la période de 2, module 5, et répétons-la jusqu'à ce que la ligne contienne douze termes; nous avons la première ligne de la Table, écrite module 5.

Au moyen de la Table de numération, associons les chiffres des deux lignes et nous avons la première ligne de la Table des puissances, écrite module 13.5.

2	4	8	16	32	64	63	61	57	49	33	1	Module 13.5
2	4	8	3	6	12	11	9	5	10	7	1	Module 13
2	4	3	1	2	4	3	1	2	4	3	1	Module 5
×				×		×				×		Chiffres de gaussien $2^2.3$

La quatrième ligne du Tableau indique les chiffres de gaussien $2^2.3$, inscrits dans cette ligne. Mettons-les de côté et prenons une nouvelle association de chiffres A, différente de celles inscrites dans la première ligne, soit 11, module 13, et 2, module 5; faisons la même opération et nous avons la deuxième ligne de la Table des puissances. Mettons de côté les associations déjà inscrites et prenons-en de nouvelles jusqu'à épuisement, et nous avons les six lignes de la Table de module 13.5, comprenant la totalité des chiffres premiers à ce nombre.

Pour donner ensuite à la Table la forme ci-dessus, dans laquelle les chiffres identiques sont inscrits dans une même colonne, ce n'est plus qu'une permutation de racines primitives.

La procédure ci-dessus peut servir de type pour la construction des Tables à lignes exclusivement complètes, c'est-à-dire dans lesquelles les exposants des facteurs premiers des indicateurs des divers modules sont égaux ou nuls.

22. La méthode ci-dessus pourrait s'étendre aux modules de trois facteurs $abc = m$, en formant les Tables de périodes de a, b, c séparément, puis une Table d'association (ab), et enfin une Table d'association $(ab)c$. L'opération se compliquerait évidemment, mais n'offrirait pas au fond un degré supérieur de difficulté. Ne voulant pas allonger indéfiniment cette exposition, et désirant mettre cependant le lecteur à même de s'exercer à ces opérations, si la chose l'intéresse, je me borne, pour le module $3.5.7 = 105$, à donner ici (*fig.* 19, 20, 21) la Table de numération et les Tables inverses, accompagnées des Tables de puissances pour 3, 5, 7; et, en outre, la Table complète des puissances pour le module 105.

Table de numération.

Fig. 19.

Mod 3.5.7.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Mod 7.	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0
Mod 5.	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1
Mod 3.	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
Mod 3.5.7.	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
Mod 7.	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0
Mod 5.	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2
Mod 3.	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
Mod 3.5.7.	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
Mod 7.	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0
Mod 5.	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
Mod 3.	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
Mod 3.5.7.	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84
Mod 7.	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0
Mod 5.	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
Mod 3.	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
Mod 3.5.7.	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	0
Mod 7.	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0
Mod 5.	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0
Mod 3.	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0

Tables de numération inverses.

TABLE (3.5)(7).

Fig. 19.

7	0					1					2				
5	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
0	0	21	42	63	84	70	91	7	28	49	35	56	77	98	14
1	15	36	57	78	99	85	1	22	43	64	50	71	92	8	29
2	30	51	72	93	9	100	16	37	58	79	65	86	2	23	44
3	45	66	87	3	24	10	31	52	73	94	80	101	17	38	59
4	60	81	102	18	39	25	46	67	88	4	95	11	32	53	74
5	75	96	12	33	54	40	61	82	103	19	5	26	47	68	89
6	90	6	27	48	69	55	76	97	13	34	20	41	62	83	104

Tables réduites de puissances pour les modules 3, 5, 7.

Fig. 20.

Indices.	1 2	1 2 3 4	1 2 3 4 5 6
Puissances.	2 1	2 4 3 1	3 2 6 4 5 1
Modules.	3	5	7

Table complète des puissances de module 105 = 3.5.7.

Fig. 21.

1	2	3	4	5	6	7	8	9	10	11	12
1											1
2	4	8	16	32	$\overline{41}$	23	46	$\overline{13}$	$\overline{26}$	$\overline{52}$	1
3	9	27	$\overline{24}$	33	$\overline{6}$	$\overline{18}$	51	48	39	12	36
4	16	$\overline{41}$	46	$\overline{26}$	1						1
5	25	20	$\overline{5}$	$\overline{25}$	$\overline{20}$						$\overline{20}$
6	36										36
7	49	28	$\overline{14}$								$\overline{14}$
8	$\overline{41}$	$\overline{13}$	1								1
9	$\overline{24}$	$\overline{6}$	51	39	36						36
10	$\overline{5}$	$\overline{50}$	25	40	$\overline{20}$						$\overline{20}$
11	16	$\overline{34}$	46	$\overline{19}$	1						1
12	39	48	51	$\overline{18}$	$\overline{6}$	33	$\overline{24}$	27	9	3	36
13	$\overline{41}$	$\overline{8}$	1								1
14	$\overline{14}$										$\overline{14}$
15											15
16	46	1									1
17	$\overline{26}$	$\overline{22}$	46	47	$\overline{41}$	38	16	$\overline{43}$	4	$\overline{37}$	1
18	9	$\overline{48}$	$\overline{24}$	$\overline{12}$	$\overline{6}$	$\overline{3}$	51	$\overline{27}$	39	$\overline{33}$	36
19	46	34	16	11	1						1
20	$\overline{20}$										$\overline{20}$
21											21
22	$\overline{41}$	43	1								1
23	4	$\overline{13}$	16	$\overline{52}$	$\overline{41}$	2	46	8	$\overline{26}$	32	1
24	51	$\overline{36}$	$\overline{24}$	$\overline{51}$	36						36
25	$\overline{5}$	$\overline{20}$									$\overline{20}$
26	46	41	16	$\overline{4}$	1						1

1	2	3	4	5	6	7	8	9	10	11	12
27	$\overline{6}$	48	36								36
28	49	7	$\overline{14}$								$\overline{14}$
29	1										1
30	$\overline{45}$	15									15
31	16	$\overline{29}$	46	$\overline{44}$	1						1
32	$\overline{26}$	8	46	2	$\overline{41}$	$\overline{52}$	16	$\overline{13}$	4	23	1
33	39	27	51	3	$\overline{6}$	12	$\overline{24}$	48	9	$\overline{18}$	36
34	1										1
35	$\overline{35}$										$\overline{35}$
36											36
37	4	43	16	$\overline{38}$	$\overline{41}$	$\overline{47}$	46	22	$\overline{26}$	$\overline{17}$	1
38	$\overline{26}$	$\overline{43}$	46	$\overline{37}$	$\overline{41}$	17	16	$\overline{22}$	4	47	1
39	51	$\overline{6}$	$\overline{24}$	9	36						36
40	25	$\overline{50}$	$\overline{5}$	10	$\overline{20}$						$\overline{20}$
41	1										1
42	$\overline{21}$	$\overline{42}$	21								21
43	$\overline{41}$	22	1								1
44	46	29	16	$\overline{31}$	1						1
45	30	$\overline{15}$	$\overline{45}$	$\overline{30}$	15						15
46	16	1									1
47	4	$\overline{22}$	16	17	$\overline{41}$	$\overline{37}$	46	$\overline{43}$	$\overline{26}$	38	1
48	$\overline{6}$	27	36								36
49	$\overline{14}$										$\overline{14}$
50	$\overline{20}$										$\overline{20}$
51	24	36									36
52	$\overline{26}$	13	46	$\overline{23}$	$\overline{41}$	$\overline{32}$	16	$\overline{8}$	4	$\overline{2}$	1

Table complète des puissances de module 105 = 3.5.7 (*suite*).

Fig. 21.

1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
$\overline{52}$	$\overline{26}$	$\overline{13}$	46	23	$\overline{41}$	32	16	8	4	2	1	$\overline{26}$	46	$\overline{41}$	16	4	1						1
$\overline{51}$	$\overline{24}$	$\overline{36}$	51	24	36						36	$\overline{25}$	$\overline{5}$	20	25	5	$\overline{20}$						$\overline{20}$
$\overline{50}$	$\overline{20}$										$\overline{20}$	$\overline{24}$	51	36									36
$\overline{49}$	$\overline{14}$										$\overline{14}$	$\overline{23}$	4	13	16	52	$\overline{41}$	$\overline{2}$	46	$\overline{8}$	$\overline{26}$	$\overline{32}$	1
$\overline{48}$	$\overline{6}$	$\overline{27}$	36								36	$\overline{22}$	$\overline{41}$	$\overline{43}$	1								1
$\overline{47}$	4	22	16	$\overline{17}$	$\overline{41}$	37	46	43	$\overline{26}$	$\overline{38}$	1	$\overline{21}$	21										21
$\overline{46}$	16	$\overline{1}$	46	$\overline{16}$	1						1	$\overline{20}$											$\overline{20}$
$\overline{45}$	30	15									15	$\overline{19}$	46	34	16	11	1						1
$\overline{44}$	46	$\overline{29}$	29	16	31	1					1	$\overline{18}$	9	48	$\overline{24}$	12	$\overline{6}$	3	51	27	39	33	36
$\overline{43}$	$\overline{41}$	$\overline{22}$	1								1	$\overline{17}$	$\overline{26}$	22	46	$\overline{47}$	$\overline{41}$	$\overline{38}$	16	43	4	37	1
$\overline{42}$	$\overline{21}$	42	21								21	$\overline{16}$	46	$\overline{1}$	16	$\overline{46}$	1						1
$\overline{41}$	1										1	$\overline{15}$	15										15
$\overline{40}$	25	50	$\overline{5}$	$\overline{10}$	$\overline{20}$						$\overline{20}$	$\overline{14}$											$\overline{14}$
$\overline{39}$	51	6	$\overline{24}$	$\overline{9}$	36						36	$\overline{13}$	$\overline{41}$	8	1								1
$\overline{38}$	$\overline{26}$	43	46	37	$\overline{41}$	$\overline{17}$	16	22	4	$\overline{47}$	1	$\overline{12}$	39	$\overline{48}$	51	18	$\overline{6}$	$\overline{33}$	$\overline{24}$	$\overline{27}$	9	$\overline{3}$	36
$\overline{37}$	4	$\overline{43}$	16	38	$\overline{41}$	47	46	$\overline{22}$	$\overline{26}$	27	1	$\overline{11}$	16	34	46	19	1						1
$\overline{36}$	36										36	$\overline{10}$	$\overline{5}$	50	25	$\overline{40}$	$\overline{20}$						$\overline{20}$
$\overline{35}$											$\overline{35}$	$\overline{9}$	$\overline{24}$	6	51	39	36						36
$\overline{34}$	1										1	$\overline{8}$	$\overline{41}$	13	1								1
$\overline{33}$	39	$\overline{27}$	51	$\overline{3}$	$\overline{6}$	$\overline{12}$	$\overline{24}$	$\overline{48}$	9	18	36	$\overline{7}$	49	$\overline{28}$	$\overline{14}$								$\overline{14}$
$\overline{32}$	$\overline{26}$	$\overline{8}$	46	$\overline{2}$	$\overline{41}$	52	16	13	4	$\overline{23}$	1	$\overline{6}$	36										36
$\overline{31}$	16	29	46	44	1						1	$\overline{5}$	25	$\overline{20}$									$\overline{20}$
$\overline{30}$	$\overline{45}$	$\overline{15}$	30	45	15						15	$\overline{4}$	16	41	46	26	1						1
$\overline{29}$	1										1	$\overline{3}$	9	$\overline{27}$	$\overline{24}$	$\overline{33}$	$\overline{6}$	18	51	$\overline{48}$	39	$\overline{12}$	36
$\overline{28}$	49	$\overline{7}$	$\overline{14}$								$\overline{14}$	$\overline{2}$	4	$\overline{8}$	16	$\overline{32}$	$\overline{41}$	$\overline{23}$	46	13	$\overline{26}$	52	1
$\overline{27}$	$\overline{6}$	$\overline{48}$	36								36	$\overline{1}$	1										1

Un coup d'œil jeté sur cette Table montre que les périodes ne se terminent pas toutes par le même chiffre, mais que les chiffres terminaux sont en nombre limité. Ce sont les chiffres 1, 36, $\overline{20}$, $\overline{14}$, 21, 15, $\overline{35}$. Un peu d'attention fait voir que les chiffres des périodes qui ont le même chiffre terminal ont avec le module le même plus grand codiviseur; ainsi

3	est le plus grand codiviseur des chiffres dont les périodes se terminent par les chiffres	36
5		$\overline{20}$
7		$\overline{14}$
3.5		21
3.7		15
5.7		$\overline{35}$

Ces périodes ont cela de remarquable que si, module 3.5.7, on divise tous les termes de la période par son dernier chiffre, on trouve encore une Table de puissances. Le nouveau module s'obtient en supprimant dans 3.5.7 les facteurs communs au module et aux termes de la période.

Cette division se fait d'ailleurs très simplement en écrivant la période dans la base du nouveau module.

10	$\overline{5}$	$\overline{50}$	25	40	$\overline{20}$	Période module 3.5.7.
10	$\overline{5}$	$\overline{8}$	4	19	$\overline{20}$	Période module 3.7.
10	16	13	4	19	1	Période sans chiffre négatif.

Tables réduites.

23. De même que plus haut pour les modules premiers, nous pouvons maintenant nous proposer de construire, relativement aux modules composés, des Tables réduites de puissances, conte-

nant juste le nombre de lignes nécessaires pour renfermer tous les nombres premiers au module et assujetties à avoir 1 pour chiffre terminal de toutes leurs lignes. La disposition générale se modifiera donc quelque peu et l'on verra apparaître des cases blanches, ce qui ne s'était pas produit jusqu'ici. Ces Tableaux sont, en réalité, des Tables de puissances des racines de l'unité.

Nous allons prendre pour exemple

$$m = 85 = 17.5,$$

où $\varphi(17) = 2^4$, $\varphi(5) = 2^2$. En construisant, comme plus haut, les deux Tables de périodes et la Table d'association, puis, procédant comme nous l'avons dit, on obtient la Table cherchée (*fig.* 22) :

Table des puissances, $m = 17.5 = 85$.

Fig. 22.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	9	27	81	73	49	62	16	48	59	7	21	63	19	57	1
82	9	58	81	12	49	23	16	37	59	78	21	22	19	28	1
29	76	6	81	31	36	24	16	39	26	11	21	14	66	41	1
56	76	79	81	54	36	61	16	46	26	74	21	71	66	44	1
.	2	.	4	.	8	.	16	.	32	.	64	.	43	.	1
.	83	.	4	.	77	.	16	.	53	.	64	.	42	.	1
.	.	.	33	.	.	.	16	.	.	.	67	.	.	.	1
.	.	.	52	.	.	.	16	.	.	.	18	.	.	.	1
.	.	.	19	.	.	.	84	.	.	.	72	.	.	.	1
.	.	.	38	.	.	.	84	.	.	.	47	.	.	.	1

Voyons maintenant ce qui se passe :

On a

$$\varphi\psi(m) = 2^3 = 8:$$

il y a huit chiffres de gaussien 2^4 dans une ligne complète; le

nombre total de ces chiffres est de 32; il y aura donc $\frac{32}{8} = 4$ lignes de 16 chiffres.

Tout carré, module 17.5, a 4 racines carrées; tout chiffre de gaussien 2^3 a pour racines carrées des chiffres de gaussien 2^4. Les lignes complètes contiennent 32 chiffres de gaussien 2^4; il y a donc, dans ces lignes, $\frac{32}{4} = 8$ chiffres de gaussien 2^3; comme il y en a 16 en tout, il en reste 8 non inscrits.

Dans une ligne, il y a $\varphi(2^3) = 2^2 = 4$ chiffres de gaussien 2^3, il y aura donc $\frac{8}{4} = 2$ lignes de 8 termes.

Dans les lignes ainsi construites seront donc compris tous les chiffres de gaussien 2^4 et tous ceux de gaussien 2^3.

Passons à ceux de gaussien 2^2 : il y en a 12 en tout. Chacun de ces chiffres est une quatrième puissance d'un chiffre de gaussien 2^4 pour $m = 17.5$, toute puissance d'indice 4 a $4 \times 4 = 16$ racines quatrièmes réelles. De plus, ces chiffres sont des deuxièmes puissances des chiffres de gaussien 2^3. Il y a donc $\frac{32}{16} = 2$ chiffres de gaussien 2^2 dans les lignes de 16 termes et 2 dans les lignes de 8 termes, total 4. Comme il y en a 12 en tout, il en reste 8 non inscrits.

Dans chaque ligne, il y en a $\varphi(2^2) = 2$; il y aura donc

$$\frac{8}{2} = 4 \text{ lignes de } 4 \text{ termes.}$$

Ces lignes, au nombre de 10, dont 4 de 16 chiffres, 2 de 8 chiffres et 4 de 4 chiffres, comprennent la totalité des chiffres premiers à $m = 17.5$.

Quant à la procédure de la construction de la Table, il semble inutile de la donner. Pour former les nouvelles lignes, on prend une des associations non inscrites dans les lignes précédentes.

24. Prenons maintenant, comme second exemple, la Table de module 13.5 (*fig.* 17) qui nous permettra de faire quelques observations concernant les colonnes à chiffres tous identiques.

Nous voyons que les colonnes d'indice (4, 8, 12) sont composées de chiffres identiques. La raison du fait est fort simple. Ces co-

lonnes contiennent les $\sqrt[3]{1}$; or

$$\varphi(13) = 2^2.3, \qquad \varphi(5) = 2^2;$$

le nombre des racines cubiques, module 13, est de 3. Module 5, $\varphi(m)$ ne contient pas 3 ou le contient avec l'exposant zéro; or $3^0 = 1$; 1 n'a donc qu'une racine cubique, qui est 1 lui-même. Le nombre des racines cubiques de 1^3, module 13.5, sera donc le produit du nombre de ces racines (module 13) par leur nombre (module 5), c'est-à-dire $3.1 = 3$. De là, il résulte clairement que les colonnes d'indice (4, 8, 12) seront composées de chiffres identiques.

Le même fait se reproduira chaque fois que les indicateurs des modules composants auront des facteurs contenus exclusivement dans certains indicateurs.

Ainsi, pour ne pas y revenir, dans $m = 3.7.11$, comme on a

$$\varphi(3) = 2, \qquad \varphi(7) = 2.3, \qquad \varphi(11) = 2.5,$$

il y aura $3.5 = 15$ colonnes à chiffres identiques, c'est-à-dire la moitié de la totalité des colonnes qui sont au nombre de

$$\psi(m) = 2.3.5.$$

Ce fait est donc une conséquence très simple de la loi générale du nombre des racines d'indice α pour un module composé ([1]).

25. Examinons enfin le cas d'un module composé de trois facteurs premiers, sur l'exemple $m = 105 = 3.5.7$. En faisant usage des Tables de périodes, de leurs associations, et procédant comme nous l'avons indiqué, on obtiendra la Table demandée. Nous la donnons ici, écrite successivement dans les modules (3.5.7), (7), (5) et (3) (*fig.* 23) :

([1]) Ce nombre est égal au produit des nombres des racines pour les modules composants.

Table de puissances de module 3.5.7.

TABLE ÉCRITE, $m = 3.5.7$.

Fig. 23.

	1	2	3	4	5	6	7	8	9	10	11	12
1	2	4	8	16	32	64	23	46	92	79	53	1
2	103	4	97	16	73	64	82	46	13	79	52	1
3	37	4	43	16	67	64	58	46	22	79	88	1
4	68	4	62	16	38	64	47	46	83	79	17	1
5		101		16		41		46		26		1
6		11		16		71		46		86		1
7		94		16		34		46		19		1
8		31		16		76		46		61		1
9		74		16		29		46		44		1
10		59		16		104		46		89		1

TABLE ÉCRITE, $m = 7$.

	1	2	3	4	5	6	7	8	9	10	11	12
1	2	4	1	2	4	1	2	4	1	2	4	1
2	5	4	6	2	3	1	5	4	6	2	3	1
3	2	4	1	2	4	1	2	4	1	2	4	1
4	5	4	6	2	3	1	5	4	6	2	3	1
5		3		2		6		4		5		1
6	2	4	1	2	4	1	2	4	1	2	4	1
7		3		2		6		4		5		1
8		3		2		6		4		5		1
9	2	4	1	2	4	1	2	4	1	2	4	1
10		3		2		6		4		5		1

Table de puissances de module 3.5.7 (*suite*).

TABLE ÉCRITE, $m = 5$.

Fig. 33.

	1	2	3	4	5	6	7	8	9	10	11	12
1	2	4	3	1	2	4	3	1	2	4	3	1
2	3	4	2	1	3	4	2	1	3	4	2	1
3	2	4	3	1	2	4	3	1	2	4	3	1
4	3	4	2	1	3	4	2	1	3	4	2	1
5	4	1	4	1	4	1	4	1	4	1	4	1
6	4	1	4	1	4	1	4	1	4	1	4	1
7	2	4	3	1	2	4	3	1	2	4	3	1
8	4	1	4	1	4	1	4	1	4	1	4	1
9	2	4	3	1	2	4	3	1	2	4	3	1
10	2	4	3	1	2	4	3	1	2	4	3	1

TABLE ÉCRITE, $m = 3$.

	1	2	3	4	5	6	7	8	9	10	11	12
1	2	1	2	1	2	1	2	1	2	1	2	1
2	1	1	1	1	1	1	1	1	1	1	1	1
3	1	1	1	1	1	1	1	1	1	1	1	1
4	2	1	2	1	2	1	2	1	2	1	2	1
5		2		1		2		1		2		1
6		2		1		2		1		2		1
7	2	1	2	1	2	1	2	1	2	1	2	1
8	2	1	2	1	2	1	2	1	2	1	2	1
9		2		1		2		1		2		1
10		2		1		2		1		2		1

Le lecteur, en comparant les trois dernières Tables, verra sans peine ce fait que la vacuité de certaines cases ne provient pas toujours du même module. Le petit Tableau suivant :

5	6	7	8	9	10	Lignes
×	.	×	×	.	×	Mod 7
×	×	.	.	×	×	Mod 3

résume la situation; les croix indiquent la vacuité des cases; on y voit que, pour les cinquième et dixième lignes, la raison de cette vacuité est double; pour les lignes 7 et 8, elle provient du module 7 et, pour les lignes 6 et 9, du module 3. Quant au module 5, toutes les cases du Tableau sont forcément garnies.

En réalité, les Tables réduites, que nous venons d'expliquer sommairement, sont des instruments destinés à résoudre le problème inverse de la formation des puissances, c'est-à-dire une équation de la forme $x^a = b$, ou encore, si l'on veut, à déterminer $\sqrt[a]{b}$. Dès lors, dans ces Tables, que représentent les cases vides? Elles répondent à une impossibilité, que nous pouvons exprimer en disant que la solution est imaginaire.

Une solution réelle, pour un module composé, correspond à une solution réelle pour chacun des modules composants; si, dans l'un quelconque de ces derniers ou dans plusieurs d'entre eux, la solution est imaginaire, elle le sera pour le module composé. Ceci deviendra visible sur le Tableau suivant (*fig.* 24) formé d'après la Table réduite de puissances (*fig.* 22) du module $17.5 = 85$:

Fig. 24.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Indices.
⊙	2	.	.	.	.	.	.	⊙	.	.	.	.	.	.	.	Situation des $\sqrt[2]{}$ des chiffres inscrits sur chaque ligne.
.	.	⊙	.	.	8	.	.	.	.	⊙	.	.	.	.	.	
.	.	.	.	⊙	.	.	.	.	32	.	.	⊙	.	.	.	
.	.	.	.	.	.	⊙	.	.	.	.	.	.	43	⊙	.	
⊙	.	.	33	⊙	.	.	.	⊙	.	.	.	⊙	.	.	.	*Id.* des $\sqrt[4]{}$.
.	.	⊙	.	.	.	⊙	.	.	.	⊙	67	.	.	⊙	.	
.	⊙	.	33	.	.	.	.	.	⊙	.	.	.	.	.	.	*Id.* des $\sqrt[2]{}$.
.	.	.	.	.	⊙	.	.	.	.	.	67	.	⊙	.	.	

La première partie du Tableau fait voir la raison de la vacuité des cases de la cinquième et de la sixième ligne.

La deuxième partie en fait autant pour les quatre dernières lignes.

Le chiffre	2 8 32 43	qui $m = 5$ s'écrit	2 3 2 3	n'étant pas un	carré	Les cases	1, 9 3, 1 5, 13 7, 15	seront vides.
	33		3		carré quatrième puissance		2, 10 1, 5, 9, 13	
	67		2		carré quatrième puissance		6, 14 3, 7, 11, 15	

Modules a^α.

26. Je me propose maintenant d'étudier le cas des modules de forme a^α, ce qui n'a pas été fait dans ce qui précède.

Le module a^α est un anomal des modules composés, en ce sens que tous les facteurs sont égaux. De l'anomalie dans la constitution du module résultent des anomalies dans les Tables de puissances. Ainsi, pour a^α, on a

$$\psi(m) = \varphi(m),$$

ce qui entraîne la conséquence que les Tables réduites de puissances de module a^α ne contiennent qu'une seule ligne, fait d'une grande importance dans les calculs.

Je dois faire également ici une autre remarque ; c'est celle indiquée par Serret dans son *Algèbre supérieure,* Vol. II, p. 78 :

« Une racine primitive g du module premier impair p est une racine primitive pour le module p^ν, ν étant > 1, lorsque $\frac{g^{p-1}-1}{p}$ n'est pas divisible par p. Au contraire g n'est pas une racine primitive pour le module p^ν quand $\frac{g^{p-1}-1}{p}$ est divisible par p. »

Ces cas sont très rares ; mais pourtant ils se présentent, et la règle de Serret permet de les reconnaître. Cette vérification faite, on est certain que toute racine primitive de module a^1 est racine primitive pour le module a^α.

Comme, dans les calculs des Tables de puissances, la grande question est d'avoir une racine primitive, je crois être agréable au lecteur en donnant ici (*fig.* 25) la Table des plus petites racines primitives, positives ou négatives, pour les modules premiers de 1 à 200. J'ai mis en regard de chaque module la décomposition en facteurs premiers de son indicateur qui, dans ce cas, est le module des indices et qui, par suite, joue un rôle considérable dans les calculs.

Fig. 25.

MODULES.	R. P.	INDICATEURS.	MODULES.	R. P.	INDICATEURS.
3	2	2^1	97	5	$2^5.3^1$
5	2	2^2	101	2	$2^2.5^2$
7	$\bar{2}$	$2^1.3^1$	103	$\bar{2}$	$2^1.3^1.17^1$
11	2	$2^1.5^1$	107	2	$2^1.53^1$
13	2	$2^2.3^1$	109	6	$2^2.3^3$
17	3	2^4	113	3	$2^4.7^1$
19	2	$2^1\ 3^2$	127	3	$2^1.3^2.7^1$
23	$\bar{2}$	$2^1.11^1$	131	2	$2^1.5^1.13^1$
29	2	$2^2.7^1$	137	3	$2^3.17^1$
31	3	$2^1.3^1.5^1$	139	2	$2^1.3^1.23^1$
37	2	$2^2.3^2$	149	2	$2^2.37^1$
41	6	$2^3.5^1$	151	$\bar{5}$	$2^1.3^1.5^2$
43	3	$2^1.3^1.7^1$	157	5	$2^2.3^1\ 13^1$
47	$\bar{2}$	$2^1.23^1$	163	2	$2^1.3^4$
53	2	$2^2.13^1$	167	$\bar{2}$	$2^1.83^1$
59	2	$2^1.29^1$	173	2	$2^2.43^1$
61	2	$2^2.3^1.5^1$	179	2	$2^1.89^1$
67	2	$2^1.3^1.11^1$	181	2	$2^2.3^2.5^1$
71	$\bar{2}$	$2^1.5^1.7^1$	191	$\bar{2}$	$2^1.5^1.19^1$
73	5	$2^3.3^2$	193	5	$2^6.3^1$
79	$\bar{2}$	$2^1.3^1.13^1$	197	2	$2^2.7^2$
83	2	$2^1.41^1$	199	$\bar{2}$	$2^1.3^2.11^1$
89	3	$2^3.11^1$			

Ces préliminaires posés, prenons comme exemple $m = 49 = 7^2$. Nous pouvons, en appliquant la méthode des cycles et partant d'une racine primitive 3, former aisément la Table des puissances. Nous la disposons ici (*fig.* 26) en lui donnant la forme d'un carré

de 36 cases, et en écrivant les chiffres de 49 dans le système de base 7.

Table de puissances de module 7^2 écrite dans le système de numération de base 7.

Fig. 26.

	1	2	3	4	5	6
0	03	12	36	44	65	61
1	43	62	46	04	15	51
2	13	42	56	34	35	41
3	53	22	66	64	55	31
4	23	02	06	24	05	21
5	63	52	16	54	25	11
6	33	32	26	14	45	01
	4	5	1	3	2	6

Observons ce qui se passe : dans chaque colonne de l'intérieur du Tableau, les chiffres de droite sont identiques, les chiffres de gauche forment une progression arithmétique dont la raison est inscrite au-dessous de la colonne. Ces raisons, d'une colonne à l'autre, se suivent dans le même ordre que les chiffres dans une Table de puissances de module 7, c'est-à-dire (3, 2, 6, 4, 5, 1) en faisant abstraction du point de départ.

L'indice de la case où est inscrit le nombre 43 est un multiple de 7 ; il en est de même de toutes les cases situées sur la diagonale partant de celle-là ; les nombres inscrits dans ces cases ne sont pas

des racines primitives; si nous les mettons de côté, tous les indices des cases des colonnes 1 et 5, premiers à $6 = 2.3$, sont premiers à $7.2.3 = 42$, module des indices; les nombres inscrits dans ces colonnes sont donc des racines primitives et toutes les racines primitives, sans exception, y sont comprises.

Maintenant, prenons un module premier plus petit que 7, soit 5, et formons les Tables de puissances de 5^1, 5^2, 5^3; nous avons l'ensemble des Tableaux suivants (*fig.* 27) :

Table de puissances de module 5^3 écrite dans le système de numération de base 5.

Fig. 27.

Indices	× 1	2	× 3	4	5	6	× 7	8	× 9	10	× 11	12	× 13	14	15	16	× 17	18	× 19	20
0	002	004	013	031	112	224	003	011	022	044	143	341	232	014	033	121	242	034	123	301
1	102	204	413	331	212	424	303	311	122	244	043	141	332	214	433	421	442	234	023	101
2	202	404	313	131	312	124	403	111	222	444	443	441	432	414	333	221	342	434	423	401
3	302	104	213	431	412	324	203	411	322	144	343	241	032	114	233	021	042	134	323	201
4	402	304	113	231	012	024	103	211	422	344	243	041	132	314	133	321	142	334	223	001
Augm.	1	2	4	3	1	2	4	3	1	2	4	3	1	2	4	3	1	2	4	3

Table de puissances, de module 5^2, écrite dans le système de numération de base 5.

Indices	1	2	3	4
0	02	04	13	31
1	12	24	03	11
2	22	44	43	41
3	32	14	33	21
4	42	34	23	01
Augm.	1	2	4	3

Table de puissances, de module 5^1.

1 2 3 4	Indices
2 4 3 1	Puissances

Pour $m = 5^3$, j'ai pris pour largeur de la Table le nombre 20 égal à $\varphi(5^2)$ module des indices de la Table des puissances de module 5^2, tout comme j'ai pris pour celle de 5^2 le nombre $4 = \varphi(5^1)$ module des indices de la Table de module 5^1. Par suite, la colonne du cadre contient des multiples de 20.

Observons ce qui se passe :

Dans la Table de module 5^3, nous avons des nombres de trois chiffres représentant les puissances écrites dans la numération de base 5. Dans chaque colonne, les deux chiffres de droite sont identiques dans toutes les cases; ceux de gauche forment une progression arithmétique dont la raison est inscrite au bas du Tableau, dans chaque colonne. Ces raisons, dans la ligne qui les contient, se succèdent dans l'ordre 2, 4, 3, 1 d'un bout à l'autre, c'est-à-dire

dans l'ordre des chiffres dans la Table des puissances de module 5^4. Ici, si nous prenons les colonnes d'indices premiers à 20 (marqués d'une croix), tous les indices des cases de ces colonnes sont premiers à

$$5^2 . 2^2 = \varphi(5^3) = 100,$$

module des indices de la Table, et tous les nombres premiers à ce module y sont compris. Les nombres inscrits dans les cases de ces colonnes sont donc des racines primitives, et toutes les racines primitives, sans exception, y sont comprises.

Admettons que l'on ait construit la première ligne de la Table et le premier nombre de la seconde ligne: *tout le reste de la Table est déterminé.* La différence des chiffres de gauche des deux premiers nombres de la première colonne donne le chiffre à insérer au bas de la colonne. Celui-ci connu, toute la ligne du bas de la Table s'écrit au courant de la plume. Cette ligne écrite, il n'y a, dans chaque colonne, qu'à ajouter au chiffre de gauche du nombre de la première ligne le chiffre du bas de la colonne et à former la progression arithmétique en descendant, puis, enfin, à répéter dans chaque colonne les chiffres de droite du nombre inscrit dans la première ligne.

Et voilà la Table construite sans calcul!

Les propositions démontrées par Serret dans son *Algèbre supérieure,* Volume II, pages 77 et suivantes, sont implicitement contenues dans ces Tableaux. Ainsi, dans chaque colonne à racines primitives, nous voyons que, si l'on prend le nombre qui a 0 pour chiffre de gauche et si on lui ajoute les multiples de 25 ou $5^2((5))$, on a tous les nombres de la colonne; que les indices seront celui de la première ligne plus les multiples de $20 = \varphi(5^2)$, c'est-à-dire $\varphi(5^2)((5))$. Les chiffres de droite sont les racines primitives de $5^2 m = 5^2$. Donc, étant connues les racines primitives de $m = 5^2$, on a toutes les autres en ajoutant $5^2((5))$, d'une façon générale $m^{n-1}((m))$ pour m^n.

Il y aurait certainement une foule de remarques intéressantes à faire; ainsi, pour le nombre des racines primitives des Tables de $m = a^\alpha$, le nombre des nombres premiers à a^α est

$$\varphi(a^\alpha) = a^{\alpha-1}\varphi(a),$$

ce qui donne le module des indices. Le nombre des nombres premiers à ce module est

$$\varphi\varphi(a^\alpha) = a^{\alpha-2}\,\varphi(a)\,\varphi\varphi(a),$$

qui est, par suite, celui des racines primitives.

Si l'on forme le Tableau suivant, nous voyons que, quand on passe de $\alpha = 1$ à $\alpha = 2$, le nombre des racines primitives est multiplié par $\varphi(a)$.

a^1	$\ldots\varphi\varphi(a)$
a^2	$\ldots\varphi(a)\,\varphi\varphi(a)$
a^3	$a\,\varphi(a)\,\varphi\varphi(a)$
a^4	$a^2\,\varphi(a)\,\varphi\varphi(a)$
..	....
a^α	$a^{\alpha-2}\,\varphi(a)\,\varphi\varphi(a)$

Quand α est supérieur à 1, en passant de α à $\alpha + 1$, le nombre des racines est multiplié par a; tout cela saute aux yeux en regardant le Tableau.

On pourrait de même observer que certaines propositions ne sont pas exclusives aux racines primitives de la période maximum, mais qu'elles s'étendent à toutes les racines primitives sans exception :

Indices	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
C	1	2	1	4	5	2	1	4	1	10	1	4	1	2	5	4	1	2	1	20
G	20	10	20	5	4	10	20	5	20	2	20	5	20	10	4	5	20	10	20	1
φ(G)	8	4	8	4	2	4	8	4	8	1	8	4	8	2	4	2	4	8	4	1
Puiss.	2	4	8	16	7	14	3	6	12	24	23	21	17	9	18	11	22	19	13	1

$\varphi(G)$.	G.	CHIFFRES DE GAUSSIEN G.	PUISSANCES ENTIÈRES.	
8	20	2, 8, 3, 12, 23, 17, 22, 13	sont des racines primitives des puissances entières d'indice.	1
4	10	4, 14, 9, 19		2
4	5	16, 6, 21, 11		4
2	4	7, 18		5
1	2	24		10
1	1	1		20.

Ainsi 4, 14, 9, 19 sont des racines primitives des carrés; 16, 6, 21, 11 des racines primitives des puissances d'indice 4; et ainsi de suite.

Nous laissons au lecteur le soin et le plaisir de lire, dans ces Tableaux et dans les figures analogues qu'il construirait pour d'autres modules a^α, les propositions qui y sont implicitement contenues.

Modules 2^n.

27. Ces modules méritent une attention spéciale; ici, l'anomalie est double; d'une part, tous les facteurs sont égaux; de l'autre,

$$\psi(m) = \frac{\varphi(m)}{2},$$

dès que $n > 2$, ce qui fait rentrer nos Tables réduites dans la catégorie des Tables à plusieurs lignes.

Considérons le module 2^6 et donnons immédiatement la Table réduite des puissances, écrite (module 2^6) et (module 2^2) (*fig.* 28):

Table réduite de puissances, de module 2^6.

Fig. 28.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	9	27	17	$\overline{13}$	25	11	$\overline{31}$	$\overline{29}$	$\overline{23}$	$\overline{5}$	$\overline{15}$	19	$\overline{7}$	$\overline{21}$	1
$\overline{3}$	9	$\overline{27}$	17	13	25	$\overline{11}$	$\overline{31}$	29	$\overline{23}$	5	$\overline{15}$	$\overline{19}$	$\overline{7}$	21	1
	$\overline{9}$		17		$\overline{25}$		$\overline{31}$		23		$\overline{15}$		7		1
			$\overline{17}$				$\overline{31}$				15				1
							31								1
							$\overline{1}$								1

Table réduite de puissances, de module 2^6, écrite module 2^2.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	1	3	1	3	1	3	1	3	1	3	1	3	1	3	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
.	3	.	1	.	3	.	1	.	3	.	1	.	3	.	1
.	.	.	3	.	.	.	1	.	.	.	3	.	.	.	1
.	.	.	.		.	.	3	.	.	.	.	.	.	.	1
.	.	.	.	.	.	.	3	.	.	.	.	.	.	.	1

Le nombre 3, racine primitive pour 2^2, est racine primitive pour le module 2^n, quel que soit n.

Le module des indices est ici

$$\psi(2^6) = \frac{\varphi(2^6)}{2} = 2^4 = 16.$$

Construisons par un procédé quelconque la première ligne et écrivons-la avec les chiffres négatifs ou positifs, suivant qu'ils sont plus grands ou moindres que 32; les lignes suivantes s'obtiennent en changeant les signes des termes de rangs 2^0, 2^1, 2^2, ..., 2^{n-3}. Il résulte de ces changements de signe des cases vides, et la raison de la vacuité est la même que pour les modules composés précédents, car, en écrivant la Table module 2^2, les chiffres sont alternativement 3 et 1 dans chaque ligne, et 3 est racine primitive (module 4).

Si l'on veut abréger le calcul, il n'y a qu'à observer que, dans la première ligne, si on la divise en deux parties égales dans chaque moitié, la somme des termes de même rang, pris en grandeur absolue, est égale à 2^{n-1} et que ces termes sont de signe contraire.

Quant au module des indices, il est 2^{n-2}, ce qui donne le nombre de termes de la ligne.

Le lecteur peut remarquer, dans la colonne de rang 2^{n-3}, que les racines carrées de l'unité sont 31, $\overline{31}$, 1 et $\bar{1}$, et, en général, $2^{n-1} \pm 1$ et $2^n \pm 1$.

Je donne ci-dessous (*fig.* 29) la Table de module 3.17, pour que le lecteur puisse remarquer sa similitude de forme avec la Table de module 2^6.

Table de puissances, de module 3.17.

Fig. 29.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
5	25	23	13	14	19	$\bar{7}$	16	$\overline{22}$	$\bar{8}$	11	4	20	$\bar{2}$	10	1
$\bar{5}$	25		13		19		16		$\bar{8}$		4		$\bar{2}$		1
	$\overline{25}$		13		$\overline{19}$		• 16		8		$\bar{4}$		2		1
			$\overline{13}$				16				$\bar{4}$				1
							$\overline{16}$								1
							$\bar{1}$								1

Même Table, écrite module 3.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
.	2	.	1	.	2	.	1	.	2	.	1	.	2	.	1
.	.	.	2	.	.	.	1	.	.	.	2	.	.	.	1
.	.	.	.	.	.	.	2	.	.	.	.	.	.	.	1
.	.	.	.	.	.	.	2	.	.	.	.	.	.	.	1

CHAPITRE III.

FONCTIONS RÉDUCTIBLES ET IRRÉDUCTIBLES.

Fonctions arithmétiques.

28. Ainsi que nous l'avons dit au début, les fonctions que nous voulons étudier ici sont des polynomes d'une seule variable, de la forme

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0,$$

dans lesquels les coefficients $a_n, a_{n-1}, \ldots, a_1, a_0$ sont des entiers, x ne pouvant aussi recevoir que des valeurs entières. Le but général qu'on se propose est de connaître les valeurs successives que prendra une telle fonction lorsque x prendra toutes les valeurs entières, par une variation discontinue; et notamment, de déterminer les valeurs de x propres à donner à $f(x)$ une valeur déterminée. Par ce mot *valeur,* il faut entendre, comme nous l'avons fait jusqu'ici, une valeur congruente, par rapport à un certain module m. Dans tout ce qui suivra, nous supposerons invariablement que *m est un nombre premier.*

Cette hypothèse nous permet, sans rien particulariser, de faire $a_n = 1$ dans l'expression qui précède. En effet, le polynome peut s'écrire

$$a_n \left(x^n + \frac{a_{n-1}}{a_n} x^{n-1} + \frac{a_{n-2}}{a_n} x^{n-2} + \ldots + \frac{a_2}{a_n} x^2 + \frac{a_1}{a_n} x + \frac{a_0}{a_n} \right),$$

et, m étant premier, et les a étant des chiffres de m, tous les quotients seront aussi des chiffres parfaitement déterminés, car a_n n'est pas nul, sans quoi la fonction considérée ne serait pas de degré n.

Si, en général, nous écrivons

$$\frac{a_k}{a_n} = \alpha_k \qquad \text{et} \qquad \varphi(x) = x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_2 x^2 + \alpha_1 x + \alpha_0,$$

nous aurons donc

$$f(x) = a_n \varphi(x),$$

en sorte qu'on passera de $\varphi(x)$ à $f(x)$ en multipliant simplement par la valeur fixe a_n. Par suite de cette observation, tous les polynomes que nous considérerons auront 1 pour coefficient de leur premier terme.

Représentation des fonctions par les espaces arithmétiques.

29. Considérons le polynome général de degré n,

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0,$$

le module étant m. Tandis qu'en Algèbre, le nombre de ces polynomes est illimité, nous en avons ici un nombre rigoureusement fini et égal à m^n, car chaque coefficient a_k est un chiffre de m, qui ne peut prendre que m valeurs différentes, et, puisqu'il y a n coefficients dans le polynome, le nombre des associations sera m^n.

Si nous imaginons maintenant un espace à n dimensions de module m, cet espace contient m^n cases, et chacune d'elles correspondra exactement à l'une des fonctions considérées. Les valeurs $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ étant assignées et déterminant une fonction particulière, nous pouvons dire que cette fonction sera représentée par la case ayant pour coordonnées $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ dans l'espace dont nous parlons.

Cette représentation, qui se voit d'elle-même pour le cas du deuxième et celui du troisième degré, qu'on se figure facilement pour les espaces supérieurs, est extrêmement avantageuse dans cette théorie des fonctions arithmétiques. Elle en opère graphiquement la classification, et nous permettra d'inscrire dans la case correspondante les particularités diverses qui nous sembleront intéressantes, concernant une fonction déterminée.

Il faut ajouter que, si certains des coefficients a_k deviennent nuls,

la classe générale des fonctions résultant de cette hypothèse pourra être représentée par un espace d'un nombre de dimensions moindre. Il est clair, par exemple, que toutes les fonctions trinomes de la forme $x^n + a_p x^p + a_0$ seront représentées dans un espace à deux dimensions.

Nous trouverons par la suite de nombreuses applications de cette représentation. Aussi nous paraît-il inutile, quant à présent, d'en donner aucun exemple. Contentons-nous de dire que, pour abréger le langage, nous assimilerons fréquemment la fonction avec la case qui la représente, en disant, par exemple, que telle fonction a pour coordonnées a_0, a_1, a_2, ..., ou que telle case admet certains facteurs. Il ne saurait en résulter aucune équivoque ni aucune obscurité, tout au contraire, une fois la convention admise.

Fonctions réductibles.

30. Soit $f(x)$ une fonction donnée. Si elle est telle qu'on ait identiquement $f(x) = f_1(x) f_2(x)$ par rapport au module m, cela signifiera qu'algébriquement on aura

$$f(x) + m\theta(x) = f_1(x) f_2(x),$$

$\theta(x)$ étant une nouvelle fonction à coefficients entiers.

Nous dirons alors que la fonction $f(x)$ est *réductible*, et qu'elle admet pour facteurs ou pour diviseurs les polynomes $f_1(x)$, $f_2(x)$ qui sont à coefficients entiers, ainsi que $\theta(x)$.

Il est clair que les fonctions $f_1(x)$, $f_2(x)$ sont nécessairement de degrés n_1, n_2 inférieurs à n, degré de $f(x)$, et qu'on aura

$$n_1 + n_2 = n.$$

En supposant que les fonctions f_1, f_2 soient elles aussi réductibles, et qu'on poursuive ainsi la décomposition en facteurs aussi loin qu'il se pourra, il est bien clair qu'on se trouvera arrêté dans ces décompositions chaque fois qu'on tombera sur un binome du premier degré, nécessairement irréductible, et que le maximum des décompositions serait représenté par la relation identique (module m)

$$f(x) = (x + \alpha_1)(x + \alpha_2)\ldots(x + \alpha_n).$$

On dirait alors que $-\alpha_1$, $-\alpha_2$, ..., $-\alpha_n$ seraient les racines de l'équation $f(x) = 0$. Ces valeurs, qui sont des entiers $((m))$, auraient en effet pour résultat, si l'on substituait à x l'une quelconque d'entre elles dans la fonction $f(x)$, de rendre celle-ci nulle (module m).

La recherche des racines, s'il en existe, et tout au moins le problème de la décomposition complète d'une fonction en facteurs, est capitale dans la théorie des fonctions arithmétiques. On comprend en effet que le problème fondamental : *trouver les valeurs de x qui donnent à la fonction connue* $F(x)$ *la valeur* A, se traduit par $F(x) = A$, ou, en posant $F(x) - A = f(x)$, par l'équation $f(x) = 0$.

C'est l'équivalent de la résolution des équations en Algèbre, et nous allons voir se révéler, entre ces deux théories, des analogies frappantes à côté de dissemblances notables.

Fonctions irréductibles.

31. Si une fonction $f(x)$ est telle qu'on ne puisse satisfaire d'aucune façon à l'identité arithmétique écrite plus haut

$$f(x) = f_1(x) f_2(x),$$

ou, ce qui revient au même, à l'identité algébrique

$$f(x) + m\theta(x) = f_1(x) f_2(x),$$

par des fonctions $f_1(x)$, $f_2(x)$ à coefficients entiers, on dit que la fonction $f(x)$ est *irréductible*.

La décomposition d'une fonction donnée en fonctions irréductibles se présente comme le problème essentiel correspondant à la résolution des équations. Alors qu'en Algèbre on peut toujours supposer le premier membre de l'équation mis sous la forme $(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$, même si nous ne pouvons résoudre algébriquement cette équation, dont les racines α sont de la forme générale $a + b\sqrt{-1}$, ici nous trouverons le moyen de déterminer les racines entières, c'est-à-dire les diviseurs du premier degré; mais, si ces racines sont en nombre inférieur au degré de l'équa-

tion, nous serons arrêtés, et nous tenterons de trouver les diviseurs irréductibles du deuxième degré, puis du troisième et ainsi de suite. Nous pourrons alors dire que la décomposition est totalement effectuée ou, si l'on veut, que l'équation $f(x) = 0$ est résolue dans la mesure où elle peut l'être. En dehors des p racines entières, par exemple, correspondant à p facteurs du premier degré, nous pourrons dire que les $n-p$ racines restantes sont imaginaires. Jusqu'à nouvel ordre, il ne faut voir dans cette manière de dire qu'un symbole d'impossibilité.

Disparition du deuxième terme.

32. Dans une équation algébrique

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_0 = 0,$$

on sait qu'on peut faire disparaître le deuxième terme, en posant

$$x = y - \frac{a_{n-1}}{n},$$

et que l'équation en y devient alors

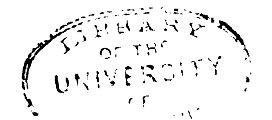
$$y^n + b_{n-2}y^{n-2} + \ldots + b_0 = 0.$$

Cette transformation est également possible dans une équation arithmétique, sauf dans le cas où le degré n serait égal à un multiple du module m ou à ce module lui-même. En effet, la relation de transformation deviendrait alors $x = y - \frac{a_{n-1}}{0}$, symbole d'une impossibilité.

Sauf cette circonstance exceptionnelle, la transformation dont il s'agit aura le très notable avantage d'abaisser d'une unité le nombre des dimensions nécessaires à l'espace représentatif de l'équation, sans porter aucune atteinte à sa généralité.

Notations, opérations.

33. Il est très commode, surtout au point de vue des calculs, de représenter une fonction arithmétique en supprimant la lettre x



et en écrivant la suite de ses coefficients dans leur ordre, suivant les puissances décroissantes.

Par exemple, soient (module 7) les deux polynomes

$$x^3 + 4x^2 + 6x + 2, \quad 5x^2 + 3x + 1;$$

nous les écrirons simplement 1462, 531. Dès lors, les opérations algébriques congruentes que nous pourrons avoir à faire s'effectueront avec une grande facilité. Nous en donnons ici un spécimen :

Addition.

```
 1462
  531
 ----
 1223
```

Soustraction.

```
 1462
  531
 ----
 1631
```

Multiplication.

```
   1462
    531
   ----
   1462
  3546
 5623
 ------
 521452
```

Division.

```
 1462 | 531
 123  |----
 ---- | 36
  232
  246
  ---
   63
```

Il nous semble inutile d'entrer dans des détails qui se comprennent d'eux-mêmes; il suffira de remarquer que les calculs sont même plus simples que ceux de l'arithmétique élémentaire, en ce sens qu'on opère chiffre par chiffre, et que, pour la division, la Table de division peut être utile si le module est un peu élevé.

Dans la représentation indiquée au n° 29 on peut noter que la case ayant pour coordonnées $a_{n-1}, \ldots, a_1, a_0$ correspond à un polynome ayant pour notation $1\,a_{n-1}, \ldots, a_1, a_0$.

Voici encore un exemple; c'est la recherche du plus grand codiviseur (module 5) entre $x^4 - 1$ et $x^3 + 3x^2 + x + 4$. Nous écrirons respectivement ces deux polynomes 10004, 1314 :

	12	2	2	4
10004	1314	341	44	11
2414				
341	044	11	0	

$x+1$ est donc le plus grand codiviseur demandé. Algébriquement, on a en effet

$$x^3+3x^2+x+4=(x+1)(x^2+2x-1)+5,$$

et la division est possible (module 5) car le reste $=0$.

Classification des polynomes des divers degrés.

34. Prenons comme exemple le module 5, et cherchons à constituer jusqu'au troisième degré, pour ne pas étendre indéfiniment les figures numériques, les diverses fonctions qu'on peut rencontrer. Le premier terme étant toujours 1, il n'y a que cinq polynomes possibles du premier degré, qui sont 10, 11, 12, 13, 14. En les combinant entre eux deux à deux de toutes les manières possibles par multiplication, nous obtiendrons des fonctions du deuxième degré, réductibles par conséquent à deux facteurs du premier degré. Ces polynomes seront représentés par la notation $1\,a_1\,a_0$, mais toutes les combinaisons de cette nature ne s'y rencontreront pas; celles qui restent représenteront donc des fonctions irréductibles du deuxième degré.

En combinant trois à trois les polynomes du premier degré, nous aurons une nouvelle catégorie. En combinant un polynome du premier degré avec un polynome irréductible du deuxième, nous en aurons encore une autre. Enfin, les polynomes du troisième degré non encore obtenus représenteront des fonctions irréductibles.

On notera que les combinaisons dont il s'agit doivent avoir lieu avec répétition, sans quoi on exclurait les racines multiples. Les six catégories que nous venons d'indiquer peuvent être représentées par P_1, $P_2^{1,1}$, P_2^1, $P_3^{1,1,1}$, $P_3^{1,2}$, P_3^1, l'indice inférieur marquant le degré, et les indices supérieurs les décompositions; l'indice supérieur 1 correspond aux fonctions irréductibles.

Les nombres des fonctions de chaque catégorie sont respectivement

$$m,\quad K_m^2,\quad m^2-K_m^2,\quad K_m^3,\quad m(m^2-K_m^2),\quad mK_m^2-K_m^3,$$

K_p^q représentant le nombre des combinaisons de p objets q à q,



avec répétition. Ces résultats, pour le module $m = 5$, se vérifieront immédiatement dans les Tableaux ci-dessous (*fig.* 30). Ils sont d'ailleurs bien faciles à établir.

Polynomes du premier degré, en nombre 5.

Fig. 30.

10	11	12	13	14

Polynomes du deuxième degré réductibles en facteurs du premier degré, en nombre 15.

100	10, 10	110	10, 11	120	10, 12	130	10, 13	140	10, 14
101	12, 13	113	12, 14	121	11, 11	131	14, 14	143	11, 13
104	11, 14	114	13, 13	122	13, 14	132	11, 12	144	12, 12

Polynomes du deuxième degré irréductibles, en nombre 10.

102	111	123	133	141
103	112	124	134	142

Polynomes du troisième degré décomposables en facteurs du premier degré, en nombre 35.

Fig. 30.

1000	10, 10, 10	1100	10, 10, 11	1200	10, 10, 12	1300	10, 10, 13	1400	10, 10, 14
1010	10, 12, 13	1130	10, 12, 14	1210	10, 11, 11	1310	10, 14, 14	1430	10, 11, 13
1040	10, 11, 14	1140	10, 13, 13	1220	10, 13, 14	1320	10, 12, 11	1440	10, 12, 12
1031	13, 13, 14	1111	11, 12, 13	1212	12, 12, 13	1301	12, 12, 14	1441	11, 14, 14
1022	12, 14, 14	1103	13, 14, 14	1243	11, 12, 14	1331	11, 11, 11	1402	11, 11, 12
1023	11, 11, 13	1123	12, 12, 12	1204	11, 13, 13	1342	11, 13, 14	1422	13, 13, 13
1034	11, 12, 12	1144	11, 11, 14	1234	14, 14, 14	1313	11, 13, 13	1414	12, 13, 14

Polynomes décomposables en facteurs du premier et du deuxième degré, en nombre 50.

Fig. 30.

1020	10, 102	1110	10, 111	1230	10, 123	1330	10, 133	1410	10, 141
1030	10, 103	1120	10, 112	1240	10, 124	1340	10, 134	1420	10, 142
1044	13, 123	1121	14, 124	1211	14, 134	1321	13, 102	1401	13, 112
1001	11, 141	1112	14, 123	1221	11, 111	1332	12, 111	1421	12, 123
1041	12, 133	1122	11, 102	1231	12, 103	1303	11, 123	1432	14, 103
1002	13, 124	1132	13, 134	1241	13, 142	1333	14, 142	1413	11, 133
1012	11, 142	1142	12, 141	1202	14, 133	1314	11, 124	1423	14, 102
1003	12, 134	1133	11, 103	1232	11, 112	1324	14, 141	1433	12, 124
1013	14, 112	1104	12, 142	1233	13, 141	1334	13, 103	1443	13, 111
1004	14, 111	1124	13, 133	1224	12, 102	1344	12, 112	1424	11, 134

Polynomes irréductibles du troisième degré, en nombre 40.

Fig. 30.

1011	1101	1201	1302	1403
1014	1102	1203	1304	1404
1021	1113	1213	1311	1411
1024	1114	1214	1312	1412
1032	1131	1222	1322	1431
1033	1134	1223	1323	1434
1042	1141	1242	1341	1442
1043	1143	1244	1343	1444

Pour passer maintenant au quatrième degré, nous devrions former les associations 4 à 4 des facteurs du premier degré, en nombre K_m^4, soit ici $K_5^4 = 70$; puis les associations de 2 facteurs du premier degré et d'un du deuxième degré irréductible, en nombre $K_m^2 (m^2 - K_m^2)$, soit $15 \times 10 = 150$; les associations des facteurs irréductibles du deuxième degré (combinaisons avec répétition) en nombre $\frac{(m^2 - K_m^2)(m^2 - K_m^2 + 1)}{2}$, ou $\frac{10.11}{2} = 55$; enfin celles des facteurs du premier degré avec les facteurs irréductibles du troisième, en nombre $m(K_m^2 - K_m^3)$ ou $5.40 = 200$.

La somme est

$$70 + 150 + 55 + 200 = 475;$$

en la retranchant des $625 = 5^4$ cases de notre espace représentatif à 4 dimensions, il nous reste 150 cases vides, où prendront place les fonctions irréductibles du quatrième degré.

En étendant de proche en proche cette façon de procéder, on comprend qu'il est possible de dresser ainsi des Tableaux comme ceux de la figure 30, donnant pour toutes les cases leurs décompositions respectives en fonctions irréductibles.

Espaces décomposants.

35. Si, dans chacune des cases de l'espace représentatif, nous inscrivons les facteurs composants dont nous venons de parler, en laissant blanches les cases irréductibles, nous obtenons une figure que nous appelons un *espace décomposant*. En même temps que la représentation des fonctions elles-mêmes, nous y voyons, sur l'emplacement de cette fonction, sa décomposition. L'intérêt de cette construction laborieuse ne serait pas considérable s'il n'offrait d'autres particularités, car la liste donnée plus haut (*fig.* 30), et donnée comme il a été dit, pourrait suffire. Mais les propriétés des espaces décomposants sont de nature à en faciliter la construction, en même temps qu'ils peuvent permettre la constatation de certaines propriétés. C'est ce qui nous décide à nous y arrêter quelques instants, en commençant par donner (*fig.* 31), pour l'étude de la fonction du quatrième degré, le cube d'argument zéro d'un espace à 4 dimensions de module 5.

Fig. 31.

	100 *ba*				
	0	1	2	3	4
0	10, 10 10, 10	102 103			14. 13 12, 11
1	10, 11 141	12 1343	13 1244	14. 14 123	
2	10. 13 124	11 1411	14 1113	12, 12 112	
3	10, 12 134	14 1114	11 1412	13, 13 142	
4	10. 14 111	13 1242	12 1341	11. 11 133	

	101 *ba*				
	0	1	2	3	4
0	10, 10 13, 12	111 141		14, 11 102	103 103
1	10 1011		14. 12 12, 12	13 1201	11, 11 134
2	10, 11 142	14, 13 133			12 1302
3	10, 14 112	12. 11 123			13 1203
4	10 1014		13, 11 13, 13	12 1304	14, 14 124

Fig. 31.

	102 *ba*				
	0	1	2	3	4
0	10, 10 102	13, 12 13, 12	14, 11 103		123 133
1	10 1021	14 1134	111 142	12, 11 124	13 1213
2	10, 14 14. 12		13 1214		11 1434
3	10. 11 13, 11		12 1311		14 1131
4	10 1024	11 1431	112 141	14. 13 134	12 1312

	103 *ba*				
	0	1	2	3	4
0	10. 10 103	14, 11 14. 11	13. 12 102		112 142
1	10, 13 14. 13		11 1443		12 1322
2	10 1032	12 1323	123 134	13. 11 111	14 1141
3	10 1033	13 1222	124 133	14, 12 141	11 1444
4	10, 12 12, 11		14 1143		13 1223

	104 *ba*				
	0	1	2	3	4
0	10. 10 11. 14	124 134		12. 13 103	102 102
1	10. 12 133	11. 13 112			14 1101
2	10 1042		11. 11 12. 11	14 1102	13. 13 141
3	10 1043		14. 14 14. 13	11 1403	12, 12 111
4	10. 13 123	12. 14 142			11 1404

Pour bien comprendre ces figures, il faut se rappeler qu'une case quelconque de l'espace à 4 dimensions représentatif de toutes les fonctions du quatrième degré serait figurée par la notation 1*dcba*, les lettres *d*, *c*, *b*, *a* étant des ((m)), ici des ((5)). Si

nous déterminons d, en le faisant par exemple comme dans la figure 31 égal à 0, nous aurons à construire le cube $10cba$. Dans ce but, donnons à c une valeur déterminée, et nous aurons à construire un carré, b et a restant seuls indéterminés. Ce sont ces cinq carrés, composant le cube par leur assemblage, que l'on voit dans la figure 31, c ayant successivement reçu les valeurs 0, 1, 2, 3, 4. Il faut ajouter que les a sont inscrits dans la ligne supérieure et les b dans la colonne de gauche du cadre.

Espaces d'invariation.

36. Si nous considérons, dans l'un quelconque de ces carrés, un facteur, celui figuré par 13, par exemple, nous le trouverons sur toutes les cases appartenant à une même direction, à partir d'une quelconque de ses positions. Cette direction est $3a + 1b$ dans tous les carrés. De même dans le cube, les facteurs 124 sont situés sur une même direction, donnée par $4a + 2b + 1c$. D'une façon générale, nous pouvons énoncer cette proposition :

Si deux cases contiennent un même facteur, toutes les cases de la ligne qu'elles déterminent le contiendront aussi.

La démonstration est tout à fait simple, au moyen de la notation qui nous sert à désigner les cases et leurs facteurs; en la présentant sur le dernier exemple que nous venons de citer, elle n'en sera pas moins générale.

Les cases 10020 et 10144 contiennent le facteur 124; cela veut dire que les polynomes

$$x^4 + 0x^3 + 0x^2 + 2x + 0$$

et

$$x^4 + 0x^3 + 1x^2 + 4x + 4$$

sont divisibles (module 5) par $x^2 + 2x + 4$. Il en sera donc de même de leur différence, qui est ici justement $x^2 + 2x + 4$. En marchant d'un pas régulier sur la ligne qui joint les deux cases, nous ne faisons qu'ajouter successivement cette différence, et par conséquent les polynomes correspondant aux cases ainsi obtenues seront tous divisibles par $x^2 + 2x + 4$.

Il y a plus. Si nous avons rencontré le facteur 124 dans *une seule case*, et si nous marchons à partir de cette case dans la direction $1c + 2b + 4a$, nous sommes assurés de rencontrer encore des cases contenant le même facteur. Cela revient en effet à cette proposition évidente : si à un polynome divisible par $x^2 + 2x + 4$, on ajoute successivement ce diviseur, on aura encore des polynomes divisibles par $x^2 + 2x + 4$.

Les lignes dont nous venons de parler, qui contiennent un même facteur, sont dites *lignes d'invariation*.

Si nous supposons maintenant trois cases, non en ligne droite, contenant un même facteur, les deux directions obtenues en joignant l'une de ces cases aux deux autres donneront deux lignes, et détermineront ainsi un espace à 2 dimensions qui contiendra encore le même facteur, et cette remarque, étendue de proche en proche, nous conduit à la proposition très importante que nous pouvons maintenant formuler :

Dans un espace décomposant à n dimensions, si ν *cases irréductibles* ($\nu < n$) *contiennent un même facteur, elles déterminent un espace à* $\nu - 1$ *dimensions dont toutes les cases contiendront aussi le même facteur* [1].

Un tel espace est dit *espace d'invariation*.

37. On comprend maintenant à quel point se trouve facilitée et simplifiée la construction d'un espace décomposant par les remarques qui précèdent. Au lieu de former toutes les combinaisons possibles de facteurs, pour les inscrire un à un, dans les cases qui correspondent à leurs produits, il suffira d'en avoir casé un seul pour en avoir immédiatement m, par une opération purement mécanique; une autre case, extérieure à la droite qui vient d'être obtenue par les m premières cases, nous déterminera un plan contenant m^2 cases, en tout, et ainsi de suite. Dans ces conditions, la construction sera donc plus ou moins longue, mais toujours exclusivement mécanique.

---

[1] Pour l'irréductibilité dans les espaces à plusieurs dimensions, voir *Esp. ar.*, Chap. III et V.



Uniformité des décompositions.

38. La méthode de synthèse employée ci-dessus nous permet d'établir maintenant une proposition fort importante, et qu'il eût été plus délicat de démontrer *a priori*, c'est qu'*une fonction arithmétique donnée ne peut être décomposée en facteurs irréductibles que d'une seule manière.*

En effet, notre espace représentatif contient toutes les fonctions possibles, et chacune d'elles une seule fois. D'autre part, toutes les combinaisons possibles de facteurs ont été faites sans aucun double emploi, et ont conduit, par les opérations uniformes de multiplication, à autant de produits différents, dont chacun indique sans ambiguïté la situation d'une case. Les facteurs composants d'une case sont donc un véritable système de coordonnées pour cette case, et celle-ci ne peut pas plus avoir deux systèmes différents de facteurs qu'un point ne peut avoir deux systèmes de coordonnées différentes, en Géométrie analytique.

Si les coordonnées sont connues, le point est déterminé; si le point est donné, les coordonnées sont déterminées.

De même, si les facteurs irréductibles sont connus, la fonction est déterminée; si la fonction est donnée, les facteurs sont déterminés.



CHAPITRE IV.

RACINES DE L'UNITÉ. IMAGINAIRES DE GALOIS

Racines de l'unité.

39. Considérons, m étant un nombre premier et n un entier, l'expression $\sqrt[m^n-1]{1}$, ou $1^{\frac{1}{m^n-1}}$. Désignant par i ce symbole, auquel provisoirement nous n'attribuerons aucune autre propriété que celle résultant de sa définition, imaginons que i soit pris comme base d'une Table de puissances (module m). Puisque $i^{m^n-1} = 1$, nous aurons $i^{m^n} = i$, par une simple convention étendant à ces expressions les règles du calcul algébrique. Dès lors, notre Table aura $m^n - 1$ termes,

$$i, \quad i^2, \quad i^3, \quad \ldots, \quad i^{m^n-1},$$

la suite de la Table reproduisant indéfiniment les mêmes termes.

La série des indices est

$$1, \quad 2, \quad 3, \quad \ldots, \quad m^n - 1.$$

Actuellement, constatons que, i étant racine de l'équation $x^{m^n-1} - 1 = 0$ (module m), il en sera évidemment de même de toutes les puissances $i^2, i^3, \ldots, i^{m^n-1}$, et regardons-les comme toutes essentiellement différentes les unes des autres. Elles sont au nombre de $m^n - 1$, et elles représentent par conséquent toutes les racines de l'équation binome $x^{m^n-1} - 1 = 0$.

On remarquera que la seule définition de i, rapprochée de l'hypothèse que les puissances de i sont toutes différentes, crée une assimilation totale entre cette suite et celle des racines *algébriques* de l'équation $x^{m^n-1} - 1 = 0$, à cette seule différence près que les relations qu'on serait amené à écrire dans ce dernier cas seraient

elles-mêmes des équations algébriques qu'on devrait ensuite transformer en équations arithmétiques de module m. Mais cette transformation ne saurait rien changer aux propriétés générales des racines de l'unité; elle nous interdit seulement de les identifier avec des expressions de la forme $\cos\alpha + \sqrt{-1}\sin\alpha$ à cause de l'introduction de nombres irrationnels qui enlèveraient aux résultats tout sens arithmétique.

De ces propriétés générales, nous allons retenir celles qui seront nécessaires à notre étude, sans avoir besoin de les démontrer par le détail, puisqu'elles sont classiques, et en donnant seulement les explications indispensables à une entière clarté.

Il n'y aura même que des avantages, si nous le voulons, à identifier les $m^n - 1$ puissances de i avec les rayons d'une circonférence partagée en $m^n - 1$ parties égales, à partir d'une certaine origine, comme cela a lieu dans la représentation des imaginaires algébriques, racines de l'équation binome.

Dans cet ordre d'idées, notre attention devra se porter spécialement sur les indices, qui sont des nombres entiers, qui ont une réalité concrète, sans que nous soyons obligés d'attribuer une signification spéciale à l'expression i^k; tout ce que nous savons, c'est que, si k devient égal à $m^n - 1$ ou à l'un de ses multiples, i^k sera égal à 1.

La distinction des racines i, i^2, ... en deux classes : celles qui sont aussi racines d'une équation binome de degré inférieur à $m^n - 1$, et les autres, qu'on appelle *racines primitives*, s'impose donc dès maintenant, et notre hypothèse que les i^k sont tous différents entraîne cette conséquence que i est une racine primitive de l'unité, d'indice $m^n - 1$.

Si ν est diviseur de n, l'identité

$$\frac{m^n - 1}{m^\nu - 1} = m^{n-\nu} + m^{n-2\nu} + \ldots + m^\nu + 1$$

nous montre que $m^\nu - 1$ sera un diviseur de $m^n - 1$, et que, par conséquent, $i^{m^\nu - 1}$ ne sera pas une racine primitive. En donnant à ν toutes les valeurs possibles pour qu'il en soit ainsi, c'est-à-dire en remplaçant ν par tous les diviseurs de n, nous arriverons à pouvoir opérer le triage et la classification de toutes les puissances de i.

Si nous décomposons $m^n - 1$, qui n'est pas premier, en ses facteurs premiers, sous la forme $a^\alpha b^\beta c^\gamma \ldots$, tous les diviseurs de $m^n - 1$ pourront être classés dans des Tables spéciales correspondant à chacun des facteurs a^α, b^β, c^γ, ... et obtenus par la combinaison de ces divers éléments. Les racines primitives relatives à chacun des facteurs sont au nombre de $\varphi(a^\alpha)$, $\varphi(b^\beta)$, ... respectivement, et celui des racines primitives de l'équation $x^{m^n-1} - 1 = 0$ sera

$$\varphi(m^n - 1) = \varphi(a^\alpha)\varphi(b^\beta), \quad \ldots.$$

Dès lors, nous pourrons, pour chacun des diviseurs δ de $m^n - 1$, séparer les racines de l'équation $x^\delta - 1 = 0$ en deux catégories, les racines primitives, et celles qui ne le sont pas. Toutes prendront place dans la Table des puissances de i.

Tous les binomes $m^\nu - 1$ dans lesquels ν est un diviseur de n, et ceux-là seulement, sont des diviseurs de $m^n - 1$, c'est-à-dire font partie de la catégorie des δ dont nous venons de parler.

Fonctions symétriques.

40. La série des puissances de i nous présentant la totalité des racines de l'équation binome $x^{m^n-1} - 1 = 0$, il s'ensuit que leur somme Σ_1, la somme Σ_2 de leurs produits 2 à 2, ... jusqu'à la somme Σ_{m^n-2} de leurs produits $m^n - 2$ à $m^n - 2$, sont nulles séparément, et que leur produit Σ_{m^n-1} est -1, le degré $m^n - 1$ étant pair. On peut vérifier directement ce dernier fait, car le produit est

$$i^{\frac{m^n(m^n-1)}{2}} = i^{\frac{m^n-1}{2}} = \sqrt{1} = \pm 1;$$

or ce ne peut pas être $+1$ qui correspond à i^{m^n-1}, donc c'est -1. Incidemment, on remarque que l'indice de -1 sera $\frac{m^n - 1}{2}$.

On peut constater aussi que les sommes des puissances $S_1 = \Sigma_1$, S_2, S_3, ... seront nulles elles aussi jusqu'à l'indice $m^n - 2$.

Pareilles remarques pourront être faites, en remplaçant n par ν, sur toutes les puissances de i qui résolvent l'équation binome $x^{m^\nu-1} - 1 = 0$, ν étant un diviseur de n.

Relation entre l'équation binome et une équation du $n^{ième}$ degré.

41. Si, au moyen des notations du Chapitre précédent, nous voulons essayer la division du polynome x^k par un polynome donné $a_{n-1}x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, on sera conduit à une division congruente complètement analogue à celle qui, en Arithmétique élémentaire, donne la conversion des fractions ordinaires en décimales et amène aux fractions périodiques.

Elle sera symbolisée par les données

$$1000\ldots\ldots\ldots\ldots \quad \Big| \; \underline{a_n a_{n-1}\ldots a_0}$$

le nombre des o du dividende étant égal à k, que pour l'instant nous laissons indéterminé, et que nous pouvons même supposer aussi grand qu'il nous plaira.

Des analogies s'imposent, que nous allons nous efforcer de constater. Pour simplifier les écritures, sans nuire en rien à la généralité des raisonnements, supposons que le diviseur soit une fonction *irréductible* du deuxième degré

$$1\,ba = x^2 + bx + a = f(x).$$

En poursuivant l'opération indiquée, nous trouverons constamment des restes de la forme $\beta\alpha$, les β, α étant des $((m))$ ainsi que b et a. Comme les combinaisons possibles de $((m))$ deux à deux sont en nombre limité, et que ce nombre est m^2, on retombera forcément, à un instant donné, sur un reste déjà obtenu, et, à partir de cet instant, l'opération prendra un caractère périodique.

Soit k la puissance de x pour laquelle le reste reproduit apparaît pour la première fois, et p le nombre de chiffres de la période. On aurait

$$x^k \quad = f(x)\,q\;(x) + \mathrm{R}(x),$$
$$x^{k+p} = f(x)\,q_1(x) + \mathrm{R}(x),$$

d'où

$$x^k(x^p - 1) = f(x)\,\mathrm{Q}(x).$$

Faisons $x = 0$; on aurait $f(x)\,\mathrm{Q}(x) = 0$; et, pour $x = 1$, il en serait de même. Or, il n'est évidemment pas possible que $\mathrm{Q}(x)$

soit nul; et, d'autre part, la fonction $f(x)$ ne peut admettre le facteur x, puisqu'elle est irréductible. En d'autres termes, la périodicité ne sera pas mixte.

Appelant toujours p le nombre des termes de la période, nous aurons alors

$$\begin{aligned} x^p &= f(x)\,q_1(x) + 1, \\ x^{2p} &= f(x)\,q_2(x) + 1, \\ &\ldots\ldots\ldots\ldots\ldots\ldots, \\ x^{\lambda p} &= f(x)\,q_\lambda(x) + 1. \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

D'un autre côté, si tous les restes apparaissent dans la division, sauf le reste oo qui est bien évidemment impossible, nous aurons $p = m^2 - 1$ (en général $m^n - 1$). Il suit de là que p ne peut être que $m^2 - 1$ ou l'un des diviseurs de $m^2 - 1$. Soit $p\delta = m^2 - 1$. Si par le symbole α nous désignons une racine de l'équation irréductible $f(x) = 0$, nous aurons

$$\alpha^p - 1 = 0, \qquad \alpha^{p\delta} = \alpha^{m^2-1} = 1.$$

Donc α sera racine de l'équation $x^{m^2-1} - 1 = 0$. Si $\delta \neq 1$ cette racine α ne sera pas primitive. Pour qu'elle coïncide entièrement avec la définition de i donnée plus haut, nous devrons donc avoir $\delta = 1$, $p = m^2 - 1$; et la conclusion très importante à laquelle nous arrivons est la suivante :

Toute racine primitive de l'équation $x^{m^n-1} - 1 = 0$ *est racine d'une équation irréductible* $f(x) = 0$, *de degré* n.

On va voir comment le même résultat, sous une autre forme, résulte des recherches de Galois sur la question.

Comme exemple très simple, nous donnons ci-dessous la division de x^k par la fonction irréductible $x^2 + x + 2$, dans l'hypothèse $m = 3$; $m^n - 1 = 8$:

100	112
210	12202110
220	
020	
200	
120	
110	
01	

On a $p = 8$. Le quotient est

$$x^6 + 2x^5 + 2x^4 + 2x^2 + x + 1.$$

Formule de Galois.

42. Galois a énoncé (*Œuvres*, p. 17) et Serret démontre (*Cours d'Algèbre supérieure*, 5e édition, t. II, p. 134) une identité fort remarquable et très importante, dans la théorie qui nous occupe. Si m est un module premier, n un entier et $f(x)$ une fonction arithmétique à coefficients entiers, on a, par rapport au module m,

$$(f(x))^{m^n} = f(x^{m^n}).$$

Il s'ensuit que, si l'une des racines de l'équation $f(x) = 0$ est α, α^{m^n} sera également une racine.

Une autre conséquence intéressante est que, si β est une racine de l'équation binome $x^{m^n-1} - 1 = 0$, d'où $x^{m^n} = x$, nous aurons

$$(f(\beta))^{m^n} = f(\beta),$$

et il s'ensuit que $f(\beta)$ sera nul, ou bien que $f(\beta)$ sera racine de l'équation binome. Si, par exemple, la fonction a été choisie de telle sorte qu'elle n'ait aucune racine commune avec l'équation binome, toutes les expressions

$$f(\beta),\quad ff(\beta),\quad fff(\beta),\quad \ldots$$

seront, comme β, des racines de cette équation binome.

Applications.

43. On verra, au Chapitre VI, comment les symboles que nous venons de définir peuvent être d'un précieux secours dans l'étude des équations arithmétiques.

Ainsi que nous l'avons indiqué en commençant le présent Chapitre, l'imaginaire i pourrait être représentée par $1^{\frac{1}{m^n-1}}$, et un terme quelconque de la suite des puissances par le symbole $1^{\frac{p}{m^n-1}}$. Le

module des indices étant $m^n - 1$, cette seule forme montre que nous sommes en présence de symboles nécessairement imaginaires, puisqu'en général l'indice l'est aussi, prenant la forme $\frac{p}{0}$. Du reste, nous ne saurions trop insister sur cette considération, que c'est surtout sur les indices que toute l'attention doit être portée. On fera les multiplications par des additions d'indices, les divisions par des soustractions, les extractions de racines par des divisions d'indices. Si cette division se trouve impossible, comme il arrive dans le cas des modules composés, l'extraction de racine sera impossible aussi. Mais, au fond, c'est dans la division que se trouve en réalité l'origine des impossibilités que nous pouvons avoir avantage à traduire par la création d'êtres arithmétiques de raison, que nous qualifions d'imaginaires. Le grand parti qu'en a tiré Galois est une preuve de l'avantage que présentent dans certains cas ces symboles, en éclairant d'une lumière nouvelle des coins obscurs de la Science, en faisant découvrir des propriétés nouvelles. C'est ainsi qu'on arrive parfois à considérer les propriétés déjà connues comme de simples cas particuliers, le réel ne devenant alors qu'une anomalie par rapport à l'imaginaire, plus général.

44. Pour achever de faire comprendre, sur un exemple numérique, les indications données plus haut, nous allons opérer le triage total des puissances de i dans le cas où $m = 5$, $n = 4$; d'où $m^n - 1 = 624$. Nous n'opérerons exclusivement que sur les indices.

Ayant écrit ces indices, de 1 à $624 = 5^4 - 1$, nous formerons d'abord l'expression

$$\frac{5^4 - 1}{5 - 1} = \frac{624}{4} = 156.$$

Elle nous montre que nous avons quatre puissances de i dont les indices sont

156 312 468 624

et que nous pourrons appeler *imaginaires du premier ordre*. On trouvera plus loin la justification en même temps que le sens précis de cette dénomination.

Formons de même $\frac{5^4-1}{5^2-1}=26$. Nous aurons vingt-quatre puissances de i, comprenant les quatre trouvées ci-dessus, et dont les indices sont

26	52	78	104	130	156
182	208	234	260	286	312
338	364	390	416	442	468
494	520	546	572	598	624

Les indices entourés 156, ... sont ceux des imaginaires du premier ordre. Il en reste 20, et nous dirons que les puissances de i correspondantes sont des imaginaires du deuxième ordre. Dans cet exemple numérique, nous ne pouvons pousser plus loin; mais on continuerait de la même manière en formant toujours les expressions $\frac{m^n-1}{m^\nu-1}$, ν étant un diviseur de n; ici $n=4$, et il n'y a pas de diviseur supérieur à 2.

Le triage des autres facteurs s'opérerait ensuite par la décomposition de 624, qui donne $2^4.3.13$. Mais ceux que nous venons de séparer ont une importance capitale. Il peut être intéressant de reproduire le Tableau ci-dessous, comprenant les indices des imaginaires d'ordre 1 et d'ordre 2, en les écrivant dans le système de numération de base 5 :

0101	0202	0303	0404	1010	1111
1212	1313	1414	2020	2121	2222
2323	2424	3030	3131	3232	3333
3434	4040	4141	4242	4343	4444

On considérera toutes les 600 autres puissances de i, après suppression de celles qui ont les indices ci-dessus, en nombre 24, comme des imaginaires du quatrième ordre.

Le Tableau général des diviseurs de 624, en supprimant 624, est :

1	3	6	12	16	26	48	78	156	312
2	4	8	13	24	39	52	104	208	

On enlèvera tous leurs multiples en supprimant ceux de 2, de 3 et de 13, et il restera 192 indices, qui sont :

1	79	157	235	313	391	469	547
5	83	161	239	317	395	473	551
7	85	163	241	319	397	475	553
11	89	167	245	323	401	479	557
17	95	173	251	329	407	485	563
19	97	175	253	331	409	487	565
23	101	179	257	335	413	491	569
25	103	181	259	337	415	493	571
29	107	185	263	341	419	497	575
31	109	187	265	343	421	499	577
35	113	191	269	347	425	503	581
37	115	193	271	349	427	505	583
41	119	197	275	353	431	509	587
43	121	199	277	355	433	511	589
47	125	203	281	359	437	515	593
49	127	205	283	361	439	517	595
53	131	209	287	365	443	521	599
55	133	211	289	367	445	523	601
59	137	215	293	371	449	527	605
61	139	217	295	373	451	529	607
67	145	223	301	379	457	535	613
71	149	227	305	383	461	539	617
73	151	229	307	385	463	541	619
77	155	233	311	389	467	545	623

Ces nombres sont premiers au module des indices, et l'opération par laquelle on les obtient est tout à fait analogue au crible d'Eratosthène.

Les puissances de i correspondantes pourraient être appelées des *imaginaires primitives du quatrième ordre*.

Si l'on prenait l'une quelconque d'entre elles, appelée j, en construisant la Table des puissances

$$j,\quad j^2,\quad \ldots,\quad j^{m^n-1},\quad \ldots,$$

on pourrait dire exactement de cette Table tout ce que nous avons dit de

$$i,\quad i^2,\quad \ldots,\quad i^{m^n-1},\quad \ldots.$$

La lettre seule serait changée, mais les propriétés resteraient exactement les mêmes.

Dénombrement des fonctions irréductibles.

15. Les considérations qui précèdent peuvent être d'un secours précieux pour l'évaluation du nombre des fonctions irréductibles. Toute Table de puissances d'imaginaires de degré n contient toutes les imaginaires d'ordre ν, diviseur de n. Si n est premier, on n'aura que des imaginaires d'ordre n et d'ordre 1. Le nombre de ces dernières est $m-1$, et l'on aura par différence $m^n - m$, nombre des imaginaires d'ordre n. A toute fonction irréductible de degré n sont attachées n imaginaires d'ordre n, comme nous le verrons plus loin. Le nombre des fonctions irréductibles est donc dans ce cas $\frac{m^n - m}{n}$.

Si n est composé, on fera le triage successif des imaginaires des divers ordres diviseurs de n. Par exemple, pour $m = 5$, $n = 4$, les diviseurs de n sont 1, 2, 4. Il y a en tout 624 termes dans la Table; 4 sont du premier ordre, 20 du deuxième; il en reste 600, et, en divisant par 4, nous avons 150 fonctions irréductibles du degré 4.

Pour voir comment peuvent s'associer ces diverses fonctions irréductibles, prenons maintenant l'exemple $m = 5$, $n = 5$, qui permet une classification un peu plus étendue, ce cas exceptionnel $m = n$ n'ayant d'ailleurs aucune influence perturbatrice sur la question qui nous occupe ici. Les nombres des fonctions irréductibles de degrés

	1	2	3	4	5
sont					
	5	10	40	150	624

Les décompositions d'une fonction du cinquième degré pourront se faire d'après les schémas suivants :

$$a(1, 1, 1, 1, 1), \quad b(1, 1, 1, 2), \quad c(1, 1, 3), \quad d(1, 4),$$
$$e(5), \quad f(1, 2, 2), \quad g(2, 3).$$

Les combinaisons se faisant d'après la formule connue des com-

binaisons complètes, nous obtiendrons pour le nombre des fonctions

(a) $\frac{5.6.7.8.9}{1.2.3.4.5} = 126;$ (b) $\frac{5.6.7}{1.2.3}\,\frac{10}{1} = 350;$

(c) $\frac{5.6}{1.2}\,\frac{40}{1} = 600;$ (d) $\frac{150}{1} = 750;$

(e) $\frac{624}{1} = 624;$ (f) $\left(\frac{5}{1}\,\frac{10.11}{1.2}\right) = 275;$

(g) $\frac{10}{1}\,\frac{40}{1} = 400.$

Comme vérification, on retrouve, en faisant la somme, 3125 ou 5^5, nombre des cases de l'espace de module 5 à cinq dimensions.

CHAPITRE V.

RECHERCHE DES RACINES RÉELLES.

Espaces résolvants.

46. Nous avons vu (Chapitre III) comment la résolution des équations arithmétiques s'obtient par l'emploi des espaces décomposants, qui donnent pour chaque équation d'un degré déterminé les facteurs composant le premier membre, dans le cas où cette décomposition est possible. Sinon, la case correspondante reste blanche, et le premier membre est une fonction irréductible.

Ici, la question, on le remarquera, ne se pose pas exactement comme en Algèbre, où l'on se propose de résoudre *une* équation. Nous cherchons simultanément à résoudre toutes les équations, en nombre limité, qui forment le groupe des équations d'un degré donné n, et cette méthode de synthèse, loin d'accroître les difficultés, simplifie au contraire le problème.

S'il s'agit uniquement, comme c'est le but du présent Chapitre, de rechercher les seules solutions réelles, cela revient à dire que nous nous bornerons aux seuls facteurs du premier degré. Si l'on rencontre le facteur $x + \alpha$, en effet, symbolisé par 1α, cela veut dire que $-\alpha$, ou $m - \alpha$ est racine.

La solution consistera dans la construction d'un espace représentatif où l'on conservera seulement les facteurs du premier degré, mais sans les répéter dans une même case lorsqu'il y a des racines multiples. Ce sont ces espaces que nous appelons *espaces résolvants*.

Nous pouvons donc définir ces espaces de la façon suivante : Si, sur un espace décomposant, nous effaçons tous les symboles de plus de deux chiffres, et tous les symboles de deux chiffres faisant

double emploi dans une même case ; si, de plus, nous remplaçons chaque facteur par la racine correspondante, le résultat obtenu sera un espace résolvant.

Il semble dès lors qu'il n'y aurait plus rien à ajouter, mais les règles à observer pour la construction simple de ces espaces, et les observations que cette construction peut permettre de constater ont assez d'intérêt pour justifier les explications qui vont suivre.

Construction des espaces résolvants.

47. Dans cette question, comme dans les autres traitées par nous, les procédés peuvent être divers, l'idée fondamentale reste la même; c'est l'application de la méthode graphique à l'étude des fonctions arithmétiques. Par *espaces,* quel que soit d'ailleurs le nombre de dimensions, il faut toujours entendre les assemblages de cases en ligne droite définis dans notre précédent Ouvrage : *Les espaces arithmétiques hypermagiques.*

Rappelons aussi que, dans un espace de module premier, si l'on prend à volonté deux cases quelconques et si on les joint par une ligne droite, toutes les cases de cette ligne y sont comprises.

Nous avons dit qu'ici nous nous en tiendrions rigoureusement aux modules premiers. Quant aux modules composés, je me contenterai de montrer dans une Note finale (Note I) comment on peut les traiter par un procédé analogue à celui des abaques.

L'espace qui représente l'équation *générale* de degré n est à n dimensions. Mais, si nous particularisons, en attribuant à certains coefficients des valeurs déterminées, le nombre des dimensions de l'espace en sera abaissé d'autant d'unités. Si par exemple nous avons la famille des équations $x^7 + dx^5 + cx^3 + bx + a = 0$, l'espace qui les représentera sera à quatre dimensions, au lieu de sept. Les coordonnées d'une case de cet espace seront a, b, c, d; et, pour caractériser une direction, nous la dénoterons uniformément par $\alpha a + \beta b + \gamma c + \delta d$, conformément aux principes de notre précédent Ouvrage cité plus haut.

48. Considérons tout d'abord l'équation binome $x^n + a = 0$, dans laquelle nous supposons $n < m$; si n était $\geqq m$, on la ramè-

nerait à un degré inférieur par le théorème de Fermat $x^{m-1} - 1 = 0$, qui donne $x^m = x$, et cela ne saurait influer en rien sur les racines réelles.

Une telle équation se résoudra, pour toutes les valeurs de a, par une simple Table de puissances, c'est-à-dire par un espace à une seule dimension. Prenons par exemple l'équation $x^7 + a = 0$, le module étant 11. En formant les puissances successives d'une racine primitive de 11 (2 par exemple), on obtient immédiatement le Tableau que voici :

x	1	2	3	4	5	6	7	8	9	10
x^7	1	7	9	5	3	8	6	2	4	10

d'où

x^7	1	2	3	4	5	6	7	8	9	10
x	1	8	5	9	4	7	2	6	3	10

Mais puisque l'équation, pour chaque racine x, doit donner $x^7 = -a$, il s'ensuit qu'en écrivant

a	10	9	8	7	6	5	4	3	2	1

la ligne x donnera les solutions de l'équation qui correspondent, chacune à chacune, aux valeurs de la ligne a. Pour plus de commodité, nous retournerons bout pour bout les deux suites, et nous obtiendrons le Tableau

a	0	1	2	3	4	5	6	7	8	9	10
	0	10	3	6	2	7	4	9	5	8	1

véritable espace à une dimension (module 11) qui résout à la fois toutes les équations $x^7 + a = 0$. Cet espace se réduit à son axe des a. Si 7, degré de l'équation, n'était pas, comme il arrive ici, premier avec 10, module des indices, il pourrait y avoir des cases blanches, et d'autres renfermant plusieurs solutions.

Revenons maintenant à l'équation ci-dessus

$$x^7 + dx^5 + cx^3 + bx + a = 0.$$

L'espace représentatif correspondant est à quatre dimensions.

L'axe des a de cet espace est celui que nous venons de construire, et servira de base fondamentale. Remarquons bien que, pour toute équation complète ou incomplète, nous pourrons toujours le construire ainsi que nous venons de le faire.

Ceci posé, nous allons rappeler, en mettant les racines elles-mêmes en évidence, le principe général qui nous a permis de construire les espaces décomposants. Nous aurons, en même temps, occasion d'insister sur certaines particularités que, pour abréger, nous avons passées sous silence.

Si une équation $f(x) = 0$ admet la racine α pour un certain système de valeurs particulières des coefficients, cela veut dire que pour ces valeurs la fonction $f(x)$ a pour diviseur $x - a$. En ajoutant à cette fonction un multiple quelconque de $(x - a)$, on aura un nouveau polynome $f(x) + \lambda(x - \alpha)$ qui aura également $x - \alpha$ pour facteur. Dans cette formule, λ peut même être une fonction de x; cela ne porte aucune atteinte à cette remarque.

Dans l'exemple qui nous occupe, il en résulte que l'équation

$$x^7 + ax^5 + cx^3 + (b + 1)x + (a - \alpha) = 0$$

aura aussi α pour racine.

Par conséquent, d et c ayant reçu des valeurs fixes, et b, a restant seuls indéterminés, si la case de l'espace à deux dimensions de coordonnées a, b représente une équation ayant α pour racine, il en sera de même pour la case de coordonnées $a - \alpha$, $b + 1$. Autrement dit, la marche $-\alpha a + 1b$ caractérisera une ligne dont toutes les cases auront encore α pour racine.

Mais dans le cas où notre équation est incomplète, et c'est ce qui a lieu dans l'exemple choisi, il peut se présenter une petite difficulté apparente. Supposons que, b ayant été fixé, il ne nous reste que les trois indéterminées d, c, a, coefficients de x^5, x^3, x^0. Nous avons un espace à trois dimensions de coordonnées d, c, a; si nous ajoutions $x - \beta$ à l'équation, β étant racine d'une case donnée, nous ferions apparaître des termes que l'équation ne contient pas; elle n'aurait plus de représentation possible dans notre espace. Mais, de $x - \beta = 0$, on conclut

$$x^2 = \beta^2, \qquad x^2 - \beta^2 = 0, \qquad x^5 - \beta^2 x^3 = 0.$$

Donc, dans l'espace à deux dimensions, d, c correspondant à



une valeur quelconque de a, si nous remplaçons d par $d+1$, c par $c-\beta^2$, la nouvelle équation aura encore β pour racine. Autrement dit, on pourra suivre sur cet espace la marche

$$-\beta^2 c + 1\,d,$$

et l'on ne rencontrera que des cases ayant toujours β pour racine.

Si, au contraire, on considérait le carré résultant d'une valeur particulière quelconque attribuée à d, alors c et a resteraient seuls variables. Une case ayant β pour racine, on a

$$x-\beta=0, \qquad x^3-\beta^3=0:$$

on passerait donc de c à $c+1$, de a à $a-\beta^3$; et la direction d'invariation serait caractérisée par $-\beta^3 a + 1\,c$. Il y a donc ici quelques précautions à prendre, bien simples d'ailleurs quand on est prévenu.

Une conséquence évidente de ce qui précède, c'est que les racines nulles ont toujours des directions d'invariation parallèles aux axes coordonnés de l'espace représentatif.

Ces explications données, voici (*fig.* 32) trois Tableaux relatifs à l'équation

$$x^7 + dx^5 + cx^3 + bx + a = 0,$$

qui permettront de vérifier les observations précédentes et qui nous donneront occasion d'ajouter quelques remarques.

Équation $x^7 + dx^5 + a \equiv 0$. Cube n° 0, face verticale du fond.

(mod 11).

Fig. 32.

a \ d	0	1	2	3	4	5	6	7	8	9	10
0	0	10	3	6	2	7	4	9	5	8	1
1	0	3	10		6	2, 4	7, 9	5		1	8
2	3, 8 0			10	4	6, 9	2, 5	7	1		
3	0	8		4	9, 10	5	6	1, 2	7		3
4	0		4, 8	9	5	10	1	6	2	3, 7	
5	0	4	9	5, 8		1	10		3, 6	2	7
6	4, 7 0	9	5		1, 8			3, 10		6	2
7	2, 9 0	5, 7		1		8	3		10		4, 6
8	5, 6 0	2	1, 7			3	8			4, 10	9
9	0	1, 6	2	7	3			8	4	9	5, 10
10	1, 10 0		6	2, 3	7			4	8, 9	5	

Équation $x^7 + cx^3 + a \equiv 0$. Cube n° 0, coupe horizontale n° 0.

(mod 11).

Fig. 32.

a \ *c*	0	1	2	3	4	5	6	7	8	9	10
0	0	10	3	6	2	7	4	9	5	8	1
1	0		10	7, 8	5, 9			2, 6	3, 4	1	
2	5, 6 0	7, 9		3, 10					1, 8		2, 4
3	0	4	2, 8		6, 10			1, 5		3, 9	7
4	0			4, 5	3	2, 10	1, 9	8	6, 7		
5	0	6, 8		9		1, 4	7, 10		2		3, 5
6	2, 9 0				1, 7	3, 6	5, 8	4. 10			
7	3, 8 0		5, 7	1, 2					9, 10	4, 6	
8	4, 7 0		1, 6			8. 9	2, 3			5, 10	
9	0	1, 3	4, 9			5	6			2, 7	8, 10
10	1, 10 0	2, 5			4, 8			3, 7			6, 9

Équation $x^7 + bx + a \equiv 0$. Lignes de base des cubes successifs.

(mod 11).

Fig. 32.

a \ *b*	0	1	2	3	4	5	6	7	8	9	10
0	0	10	3	6	2	7	4	9	5	8	1
1	0	8	2, 4 10	5					6	1, 7, 9	3
2	2, 9 0		6, 7	10	8			3	1	4, 5	
3	0		9		3, 5 10	4	7	1, 6, 8		2	
4	0	3, 4, 6			9	10	1	2			5, 7, 8
5	0		8	7		1, 2, 5	6, 9 10		4	3	
6	5, 6 0			2	1, 4	8	3	7, 10	9		
7	4, 7 0	2		1, 3		6	5		8, 10		9
8	3, 8 0	5, 9	1		7			4		10	2, 6
9	0	1		4, 8, 9	6			5	2, 3, 7		10
10	1, 10 0	7	5			3, 9	2, 8			6	4

Pour bien se rendre compte de l'espace représentatif dont il est question et attribuer aux titres des figures un sens précis et clair, on peut supposer que, dans l'expression

$$x^7 + dx^5 + cx^3 + bx + a,$$

b indique le rang du cube, d le rang de la coupe, c le rang de la ligne et a le rang de la case. C'est ce qui a été fait pour les construire.

Prenons le premier Tableau de la figure 32 ci-dessus, résolvant l'équation $x^7 + dx^5 + a = 0$. Les lignes d'invariation, α étant une racine quelconque, sont données par $-\alpha^5 x + 1\,d$.

Tous les chiffres qui ont un même chiffre pour 5e puissance auront pour lignes d'invariation des lignes parallèles; elles ne se couperont donc nulle part dans toute l'étendue du plan. Ainsi, comme

$$(1, 3, 4, 5, 9) \quad \text{sont racines de l'équation} \quad x^5 = 1$$

et

$$(2, 6, 7, 8, 10) \quad » \quad » \quad x^{10} = 1,$$

les lignes d'invariation de la première parenthèse appartiendront à la direction $-1\,a + 1\,d$, et ceux de la seconde parenthèse à la direction $-10a + 1\,d$, ou $1\,a + 1\,d$.

Les lignes d'invariation non parallèles se couperont deux à deux en un point et en un seul, de sorte que, dans toute l'étendue du Tableau, on trouvera dans une même case un chiffre quelconque de la première parenthèse, groupé avec un chiffre quelconque de l'autre; mais nulle part on ne trouvera groupés ensemble deux chiffres d'une même parenthèse.

Ces particularités résultent de ce que le degré 5 de x a 5 pour plus grand codiviseur avec le module 10 des indices, m étant 11.

Les deux autres Tableaux de la figure résolvent les équations

$$x^7 + cx^3 + a = 0 \quad \text{et} \quad x^7 + bx + a = 0.$$

Les exposants du terme moyen étant 3 et 1, qui ont 1 pour plus grand codiviseur avec le module 10 des indices, on trouvera dans une case de chacun de ces Tableaux tous les groupements possibles de deux chiffres quelconques.

On peut remarquer qu'un plan contient m^2 chiffres et m^2 seulement, en y comprenant 0.

49. En appliquant et en étendant notre principe général de construction des espaces résolvants, il est aisé d'arriver à la notion d'un espace d'invariation d'ordre supérieur à une ligne, jusqu'à un espace à $n-1$ dimensions, auquel nous arrivons tout de suite. Pour plus de simplicité, considérons l'équation générale du troisième degré, et supposons qu'une racine α appartienne à deux cases différentes $(a_1, b_1, c_1)(a_2, b_2, c_2)$. L'équation étant

$$x^3 + cx^2 + bx + a = 0,$$

nous aurons

$$\alpha^3 + c_1\alpha^2 + b_1\alpha + a_1 = 0,$$
$$\alpha^3 + c_2\alpha^2 + b_2\alpha + a_2 = 0,$$

et, si nous appelons c, b, a les différences $c_2 - c_1$, $b_2 - b_1$, $a_2 - a_1$ qui caractérisent la direction d'invariation allant de la première case à la seconde,

$$c\alpha^2 + b\alpha + a = 0.$$

Ceci peut être considéré, pour chaque valeur de α, comme l'équation d'un plan d'invariation; et, en général, on obtiendra ainsi un espace d'invariation à $n-1$ dimensions.

Supposons, par exemple, $m = 7$ et $\alpha = 3$; d'où $\alpha^2 = 2$; il vient alors

$$2c + 3b + a = 0.$$

Qu'on prenne alors un système quelconque de valeurs de c, b, a, $c = 5$, $b = 4$, $a = 6$, par exemple, satisfaisant à cette relation. Si, à la notation d'une case quelconque contenant la racine 3, nous ajoutons 546, nous trouvons l'indication d'une case qui aura également 3 pour racine.

Ainsi, la case 1540 est dans ce cas; l'addition nous donne 1316; donc la case 1316 aura la racine 3.

Algébriquement, cela pourrait se traduire en disant que les équations arithmétiques

$$x^3 + 5x^2 + 4x \qquad = 0,$$
$$5x^2 + 4x + 6 = 0,$$
$$x^3 + 3x^2 + x + 6 = 0$$

ont toutes pour racine 3.



Ces espaces d'invariation, et en particulier les plans d'invariation, peuvent être d'un grand secours pour la construction effective des espaces résolvants, qui se résumera essentiellement en ceci : par l'annulation de tous les coefficients, sauf un, construire un des axes de l'espace, l'axe des a par exemple. Par chaque case de cet axe, contenant une racine, faire passer un espace d'invariation, un plan par exemple; et, disposant de l'indétermination des coefficients, déterminer des systèmes satisfaisant à l'équation de l'espace d'invariation. Cela permettra de trouver pratiquement et très rapidement autant de cases qu'on voudra contenant la même racine.

Abaissement du nombre des dimensions de l'espace résolvant.

50. Nous avons rappelé précédemment comment, dans une équation arithmétique, aussi bien que dans une équation algébrique, on pouvait faire disparaître le deuxième terme, à la seule condition que le degré n ne soit pas égal à m ou à l'un de ses multiples. Nous avons indiqué aussi que le degré, à l'aide du théorème de Fermat, pouvait toujours être rendu inférieur à m, tant qu'il ne s'agit que de racines réelles. Donc la transformation très simple dont il s'agit, et qui consiste à remplacer x par $x - h$, est toujours possible ([1]). Il s'ensuit qu'on ne porte aucune atteinte à la généralité de la question en faisant cette transformation préalable, et en substituant la famille d'équations

$$x^n + a_{n-2}x^{n-2} + \ldots + a_0 = 0,$$

à la classe primitivement écrite.

Elles seront au nombre de m^{n-1} seulement et se représenteront dans un espace à $n - 1$ dimensions au lieu de n. La question se trouvera ainsi considérablement simplifiée. Toutes les équations du troisième degré, par exemple, sont résolubles par un Tableau

([1]) Il y a cependant une restriction à faire, lorsque $n = m$ ou un multiple de m. C'est pour cela qu'en principe nous avons supposé $n < m$.

plan de m^2 cases, et l'espace résolvant se construira et se verra complètement, avec la plus grande facilité, par les moyens indiqués ci-dessus.

Racines multiples.

51. Il peut être intéressant de dire quelques mots des racines multiples que présentent les équations arithmétiques. Ici, exactement comme en Algèbre, une racine multiple est caractérisée par le fait qu'elle appartient en même temps, avec un degré de multiplicité moindre de 1, à l'équation dérivée. Nous savons, en effet, que l'équation $f(x) = 0$ revient à l'équation algébrique

$$f(x) + m\,\theta(x) = 0.$$

Si

$$f(x) = (x-\alpha)^{\mu}\,\varphi(x),$$

on aura

$$f'(x) = \mu(x-\alpha)^{\mu-1}\,\varphi(x) + (x-\alpha)^{\mu}(x),$$

et l'équation dérivée sera de la forme

$$(x-\alpha)^{\mu-1}\,Q(x) + m\theta'(x) = 0.$$

Les deux équations arithmétiques seront donc de la forme

$$(x-\alpha)^{\mu}\,\varphi(x) = 0, \qquad (x-\alpha)^{\mu-1}\,Q(x) = 0,$$

ce qui démontre la proposition.

Il est à noter, si paradoxale que la chose puisse paraître, que la construction indiquée dans ce Chapitre, pour les espaces résolvants, ne fait apparaître chaque racine qu'une seule fois dans une case. Il en résulte que les racines multiples se trouvent signalées graphiquement, du moins pour les degrés peu élevés, précisément à cause de l'absence des facteurs.

Bien que nous devions étudier le cas du deuxième degré dans un Chapitre spécial, nous croyons utile, à l'appui de cette observation, de donner ici (*fig.* 33) l'espace résolvant très simple de l'équation du deuxième degré (module 7).

Les cases blanches représentent les fonctions irréductibles, et les chiffres uniques soulignés sont les racines doubles.

Fig. 33.

a \ b	0	1	2	3	4	5	6
0	$\underline{0}$			2. 5		3. 4	1. 6
1	0. 6	2. 4	$\underline{3}$			1. 5	
2	0. 5	$\underline{6}$			1. 4		2. 3
3	0. 4		5. 6	1. 3	$\underline{2}$		
4	0. 3		1. 2	4. 6	$\underline{5}$		
5	0. 2	$\underline{1}$			3. 6		4. 5
6	0. 1	3. 5	$\underline{4}$			2. 6	

Pour s'assurer de la multiplicité des racines d'une équation déterminée, le mieux sera d'appliquer la méthode algébrique indiquée plus haut, en la simplifiant, au point de vue des calculs, par l'emploi des notations employées et par les réductions qu'entraînent les opérations modulaires.

Ainsi, soit (module 11) l'équation

$$x^3 - x + 6 = 0.$$

Nous écrirons le premier membre

$$10(10)6.$$

La dérivée s'obtient en écrivant

$$3,\ 2,\ 1$$

et, formant les produits,

$$30(10).$$

Cherchons le plus grand codiviseur entre 10(10)6 et 30(10);

on a

$$30(10) \times 4 = 107 \qquad\qquad 36 \times 4 = 12$$

10(10)6	107
0 3 6	10

107	12
97	19
0	

Le plus grand codiviseur est 12, c'est-à-dire $x + 2$; la racine double est -2 ou 9.

Observation sur l'emploi des dérivées.

52. Il est indispensable de prendre quelques précautions spéciales dans l'emploi des dérivées, lorsqu'il s'agit d'équations arithmétiques. Pour le faire comprendre, prenons d'abord l'exemple bien simple de la fonction $(x + 2)^3$, en supposant que le module soit 3. On aura

$$(x + 2)^3 = x^3 + 6x^2 + 12x + 8 = x^3 + 2.$$

Si nous prenons la dérivée de $(x + 2)^3$, nous avons $3(x + 2)^2$ et celle de $x^3 + 2$ est $3x^2$. Ces deux résultats sont nuls par rapport au module 3 et de formes très différentes. La valeur $x = -2$, racine multiple de l'équation $(x + 2)^3 = 0$, n'annule plus la dérivée, à proprement parler, puisque celle-ci est constamment nulle.

Il y a donc ici un défaut d'analogie entre l'Arithmétique et l'Algèbre. La relation algébrique $f(x) = g(x)$ signifie, en Arithmétique,

$$f(x) = g(x) + m\,\varphi(x).$$

De là on pourra bien conclure

$$f'(x) = g'(x);$$

mais, si la dérivation a pour résultat de faire apparaître le facteur m dans certains termes, cette identité pourra se réduire à $0 = 0$, c'est-à-dire ne rien donner, comme cela arrive dans l'exemple ci-dessus.

En Algèbre, la dérivée de tout polynome de degré n est de degré $n - 1$. En Arithmétique, la dérivée peut être d'un degré

inférieur à $n-1$ et même identiquement nulle. Réciproquement, si une dérivée est nulle, la fonction primitive est constante; ce principe algébrique n'est plus vrai en Arithmétique; si $f'(x)=0$, $f(x)$ peut être de la forme

$$F[(\varphi_1(x))^m, \varphi_2(x)^m, \ldots],$$

les polynomes F, φ_1, φ_2, ... étant arbitraires.

C'est, au fond, la raison pour laquelle on a introduit en principe l'hypothèse $n<m$; car alors, m étant premier, les dérivations ne sauraient amener le coefficient m devant aucun terme. Lorsque $n \geqq m$, il faudra donc toujours y regarder de très près.

CHAPITRE VI.

RECHERCHE DES RACINES IMAGINAIRES.

Usage des imaginaires de Galois.

53. Nous invoquerons souvent ici les considérations exposées au Chapitre IV, et qui nous fourniront tous les éléments pour la résolution complète des équations arithmétiques.

Rappelons en effet sommairement où en est maintenant le problème. Par le mécanisme des espaces décomposants, nous sommes parvenus à décomposer toutes les fonctions qui sont décomposables. Les cases blanches de l'espace répondent à des fonctions irréductibles. Plus spécialement, par les espaces résolvants, nous avons isolé les facteurs du premier degré. Il en résulte que pour une équation quelconque nous sommes en fin de compte ramené à la résolution d'une équation irréductible du degré supérieur au premier, et dont nous dirons qu'elle a ses racines imaginaires, par opposition avec les racines réelles, ou chiffres entiers, qui correspondent aux facteurs du premier degré.

Ce sont précisément les symboles créés par Galois et étudiés au Chapitre IV, qui vont nous apporter la représentation complète de ces racines imaginaires, objet de notre recherche actuelle.

Reprenons l'identité de Galois, déjà signalée plus haut,

$$(f(x))^{m^n} = f(x^{m^n}).$$

Elle est arithmétique, et suppose qu'on ait pour module m, mais tout à fait générale, c'est-à-dire indépendante du degré n. Si l'on y fait $n = 1$, elle devient

$$(f(x))^m = f(x^m).$$

Sous cette forme, elle nous montre que, si une racine de l'équation $f(x) = 0$ est représentée par i, l'expression i^m sera aussi une racine. Mais l'application de ce résultat à i^m montre que i^{m^2} sera encore une racine, et ainsi de suite. Alors, la suite

$$i, \quad i^m, \quad i^{m^2}, \quad \ldots, \quad i^{m^{n-1}}$$

représentera des racines de l'équation $f(x) = 0$.

Comme nous avons établi (11 et suiv.) que, dans l'étude des imaginaires de Galois, l'expression i est racine d'une certaine équation irréductible de degré n, et qu'en même temps i est racine primitive de l'équation binome $x^{m^n-1} - 1 = 0$, il s'ensuit que nous pouvons identifier absolument la lettre i que nous employons ici avec la même lettre employée au Chapitre IV. Nous aurons donc

$$i^{m^n-1} = 1, \quad i^{m^n} = i,$$

et la suite complète des racines de l'équation $f(x)$ sera

$$i, \quad i^m, \quad i^{m^2}, \quad \ldots, \quad i^{m^{n-1}},$$

le terme suivant i^{m^n} étant i, c'est-à-dire le premier terme d'une nouvelle période qui se reproduirait indéfiniment.

Elles sont d'ailleurs toutes différentes les unes des autres, par définition même, puisque nous avons supposé que i était une racine primitive de l'équation binome. D'ailleurs la suite totale

$$i, \quad i^2, \quad i^2, \quad \ldots, \quad i^{m^n-1}$$

comprend elle-même des termes tous différents les uns des autres.

Réalité des fonctions symétriques.

54. Appelons

$$i_1, \quad i_2, \quad \ldots, \quad i_n$$

les différentes racines de l'équation $f(x) = 0$.

Comme cette équation par hypothèse a des coefficients entiers, et que nous pouvons l'écrire comme en Algèbre, soit

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0 = 0,$$

soit

$$(x - i_1)(x - i_2)\ldots(x - i_n) = 0,$$

il en résulte que les fonctions symétriques σ_1, σ_2, σ_n qui représentent respectivement la somme, la somme des produits 2 à 2, 3 à 3, ..., $n-1$ à $n-1$, et le produit, seront respectivement

$$-a_{n-1}, \quad +a_{n-2}, \quad \ldots, \quad \pm a_0.$$

Ces fonctions symétriques sont donc toutes des chiffres du module, des nombres entiers, exclusivement réels.

Si l'on prenait, sur la suite, des i quelconques, et si l'on formait le produit des binomes $x - i_k$ entre eux, on aurait le premier membre d'une équation dont les i choisis seraient bien des racines; mais cette équation serait elle-même à coefficients imaginaires, et non plus réels.

Équation réductrice.

55. Nous avons dit que i est racine d'une certaine équation irréductible de degré n. Supposons que ce soit justement l'équation $f(x) = 0$ que nous venons de considérer. Il s'ensuit qu'on aura

$$i^n + a_{n-1}i^{n-1} + \ldots + a_1 i + a_0 = 0.$$

De là

$$i^n = -(a_{n-1}i^{n-1} + \ldots + a_1 i + a_0).$$

Lorsque, dans un calcul quelconque, nous rencontrerons la lettre i élevée à une puissance supérieure à $n-1$, nous pourrons la remplacer par un polynome en i, toujours de degré inférieur à n en fin de compte.

C'est cette transformation capitale qui permet de soumettre ces symboles au calcul, en particulier d'en dresser des Tables de puissances. Elle nous montre en outre que toute fonction de i prendra finalement la même forme, celle d'un polynome de degré $n-1$ ou de degré inférieur.

Ces polynomes différents sont en totalité au nombre de m^n, puisqu'ils résultent de toutes les associations possibles de

$$(a_0, a_1, \ldots, a_{n-1})$$

et que chaque a est un $((m))$. D'un autre côté nous avons supposé que toutes les puissances de i

$$i,\quad i^2,\quad \ldots,\quad i^{m^n-1}$$

sont différentes les unes des autres. Donc ce Tableau des puissances comprend toutes les fonctions de i, la combinaison

$$(0, 0, \ldots, 0),$$

qui ne répond à aucun polynome, restant seule en dehors.

Nous allons trouver plus loin des exemples d'application de ce procédé de calcul.

L'équation $f(x) = 0$ qui sert à abaisser toutes les puissances de i au-dessous du degré n est appelée *équation réductrice*. Le polynome par lequel i^n doit être remplacé dans les calculs est dit *fonction réductrice*.

Ainsi, avec nos notations, $f(x) = 0$ est l'équation réductrice, et $x^n - f(x)$ est la fonction réductrice ([1]).

Propriété des racines d'une équation irréductible.

56. Soit k l'indice d'une racine quelconque d'une équation irréductible de degré n. D'après ce qui précède, tous les indices des n racines seront

$$k,\quad km,\quad km^2,\quad \ldots,\quad km^{n-1}.$$

Si k a le plus grand codiviseur C avec le module des indices $\mathfrak{M} = m^n - 1$, tous les autres indices auront avec $\mathfrak{M}$ le même plus grand codiviseur, car m et $m^{n-1} - 1$ sont évidemment pre-

---

([1]) Il est intéressant de rapprocher ceci de la théorie des imaginaires algébriques. Si l'on supposait que l'équation réductrice fût $x^2 + 1 = 0$, le degré étant 2, on voit que dans le calcul il faudrait remplacer partout i^2 par -1, et que les seuls résultats obtenus seraient des polynomes du premier degré en i, par conséquent de la forme $a + bi$. On sait du reste que Cauchy a édifié une doctrine des imaginaires fondée sur la division algébrique en prenant pour module $i^2 + 1$.

La grosse différence entre les deux théories, arithmétique et algébrique, ici comme toujours, consiste en ce que dans l'une le nombre des objets quelconques considérés est toujours limité, tandis que dans l'autre il est indéfini.

miers entre eux. En vertu de la formule $\mathfrak{M} = CG$, dont nous avons déjà plusieurs fois fait usage, nous voyons que le gaussien $G = \frac{\mathfrak{M}}{C}$ sera le même pour toutes les valeurs k, km, ..., et cela nous conduit à cette proposition importante :

Toutes les racines d'une équation irréductible sont des i de même gaussien.

Il s'ensuit que, si une racine de l'équation considérée est racine primitive de l'équation binome $x^{m^n-1} - 1 = 0$, toutes les autres racines de la même équation jouiront de la même propriété. Toutes auront $\mathfrak{M}$ pour gaussien.

Imaginaires des différents ordres.

57. Si nous nous reportons aux espaces décomposants définis Chapitre III, nous savons que les cases qui restent blanches représentent des fonctions irréductibles. Par exemple, pour le degré $n = 2$, nous trouverons toutes les décompositions de la forme $(x - \alpha)(x - \beta)$ ou symboliquement 1.1, et les cases vides seront des fonctions irréductibles du deuxième degré.

Pour $n = 3$, nous aurons les décompositions 1.1.1, les décompositions 1.2, et il nous restera, vides, les cases correspondant aux fonctions irréductibles du troisième degré.

Pour n quelconque, il nous resterait les fonctions irréductibles du $n^{\text{ième}}$ degré, après avoir épuisé toutes les décompositions possibles.

Parmi ces racines du $n^{\text{ième}}$ degré, il y en a qui ont la propriété d'engendrer la Table complète des puissances de i, en élevant l'une des racines à ses puissances successives. D'autres ne jouissent pas de cette propriété, mais toutes sont résolues par des fonctions rationnelles de i, que nous appelons *imaginaires du $n^{\text{ième}}$ ordre*. A l'inverse de ce qui se passe en Algèbre, les imaginaires se trouvent donc groupées par familles, chacune résolvant les équations irréductibles de même degré.

Nous aurons ainsi des imaginaires de tous les ordres imagi-

nables, du quatrième, du troisième, du deuxième ordre, par exemple.

Or, si l'on construisait l'espace à une dimension représentant les équations du premier degré, et si nous voulions en faire un espace décomposant, toutes les cases resteraient vides, au nombre de $m-1$, car aucune décomposition n'est évidemment possible.

On peut donc dire que les entiers, qui résolvent les équations du premier degré, toutes irréductibles, sont des imaginaires du premier ordre. Cette extension est même utile à une compréhension entière et complète des symboles dont nous nous occupons.

La Table complète des m^n-1 puissances de i contiendra dans son ensemble toutes les imaginaires d'ordre n et d'autres d'ordres inférieurs à n.

Ces imaginaires d'ordres moindres que n seront d'ordre ν, le nombre ν étant un diviseur quelconque de n. Toutes les imaginaires de ces ordres ν seront dans la Table et il n'y aura pas d'autres ordres.

Si, sur la même Table de puissances, on prend un terme d'ordre ν, ce sera la racine d'une équation irréductible de degré ν; et parmi les termes, racines de cette équation, il n'y en aura que ν distincts, qui se répéteront chacun $\frac{n}{\nu}$ fois. La fonction de degré n correspondant aux indices $k, km, \ldots, km^{n-1}$, k étant l'indice du premier terme choisi, contiendra $\frac{n}{\nu}$ fonctions identiques irréductibles de degré ν. Autrement dit, on aura ainsi la décomposition d'une fonction réductible en facteurs égaux; et celle-ci aura un facteur commun avec sa dérivée.

Il est à remarquer que cette théorie de Galois amène à cette conséquence qu'une équation a autant de racines, réelles ou imaginaires, qu'il y a d'unités dans son degré, exactement comme en Algèbre.

Comme 1 est diviseur de tout nombre, une Table de puissances d'imaginaires contiendra toutes les imaginaires du premier ordre, c'est-à-dire, d'après nos observations précédentes, les $m-1$ nombres $1, 2, \ldots, m-1$.

Il résulte de tout ceci que, si l'on prend sur la Table des puissances de i les termes d'indices k, km, $\ldots$, km^{n-1}, résolvant une équation de degré n, les fonctions symétriques de ces

termes seront des entiers, c'est-à-dire des imaginaires du premier ordre, ainsi que nous l'avons fait remarquer plus haut.

Si, au contraire, les termes choisis n'obéissent pas à la loi de formation indiquée, il n'en sera plus de même et, l'équation ayant ces termes pour racines aura des coefficients imaginaires. Il faut remarquer que, dans ce cas, les coefficients ne pourront être que des fonctions d'imaginaires d'ordres ν. Par exemple, une équation du sixième degré ne pourrait être résolue que si ses coefficients étaient fonctions d'imaginaires du sixième, du troisième et du deuxième ordre, en dehors des entiers, imaginaires du premier ordre.

Bien que notre étude ne vise en principe que les équations à coefficients entiers, la remarque précédente a une assez grosse importance. On sait, en effet, que l'Algèbre permet de résoudre par radicaux les équations des deuxième, troisième et quatrième degrés. Les formules qui donnent les racines sont des Tableaux d'opérations, complètement indépendants de la nature des coefficients. Ces formules seraient donc applicables, théoriquement, à la résolution des équations à coefficients imaginaires dont nous venons de parler.

Quant aux autres, c'est à la méthode par synthèse qu'il faudra recourir, comme nous l'avons fait jusqu'ici. Cette méthode se résume complètement ici dans la construction de la Table complète des puissances de i, comme nous allons le montrer. C'est donc de la construction de ces Tables de puissances qu'il faut s'occuper maintenant.

Construction des Tables de puissances d'imaginaires.

58. Supposons qu'en prenant comme équation réductrice (55) une certaine équation

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = x^n - \varphi(x) = 0,$$

nous ayons construit une Table complète de puissances de i en partant, par conséquent, de la relation

$$i^n = \varphi(i),$$

qui permettra d'exprimer tous les termes par des polynomes en i, de degré $n - 1$ au plus.

A chaque terme différent i^k correspond un certain polynome $\varphi(i)^k = \varphi_k(i)$, et tous les polynomes φ_k sont différents les uns des autres. Connaissant donc $i^k = \varphi_k(i)$, il s'agit maintenant de déterminer l'équation qui admet cette racine. Nous savons que ses autres racines s'obtiennent en prenant les termes qui ont pour indices

$$km, \quad km^2, \quad \ldots, \quad km^n,$$

c'est-à-dire les polynomes φ correspondants, au nombre de n en tout. Si nous formions les fonctions symétriques de ces divers polynomes, savoir leur somme, la somme de leurs produits 2 à 2, ..., jusqu'à leur produit, nous obtiendrions des entiers, qui seraient, avec alternance des signes, les coefficients de l'équation cherchée, dont i^k est racine. On arrive au même résultat, par une seule opération, en formant le produit algébrique

$$(x - \varphi_1)(x - \varphi_2)\ldots(x - \varphi_n) \quad (^1),$$

dans lequel on abaissera toujours le degré de i au-dessous de n, au moyen de l'équation $i^n = \varphi(i)$.

On obtiendra ainsi l'équation cherchée, dans laquelle les coefficients, comme vérification, devront tous être réels.

Ainsi, la Table complète de puissances d'imaginaires étant dressée, on a le Tableau de toutes les racines, avec, pour chacune, l'équation que cette racine résout, équation déterminée comme nous venons de le dire ([2]).

Toute la question, dès lors, est de pouvoir construire la Table, c'est-à-dire de trouver une équation réductrice dont les racines soient primitives. On y parvient par un tâtonnement raisonné, et par quelques remarques permettant d'exclure certaines équations *a priori*.

([1]) Ici, pour simplifier, nous écrivons les indices 1, 2, ..., n au lieu de k, km, ..., km^{n-1}. Il n'en saurait résulter aucune confusion.

([2]) On pourrait encore, pour trouver l'équation dont i^k est racine, remarquer qu'elle aura pour racines les puissances $k^{\text{ièmes}}$ des racines de l'équation réductrice connue $f(x) = 0$; donc, entre cette équation et $y = x^k$, il suffira d'éliminer x pour obtenir l'équation cherchée $F(y) = 0$.

Il faut aussi, et avant tout, que le premier membre de l'équation réductrice soit une fonction irréductible. Pour ne pas nous embarrasser de questions complexes, nous ne reviendrons pas sur ce point, qui est d'ailleurs complètement élucidé par la théorie des espaces décomposants. Ces espaces nous ont permis de classer à part (cases blanches) les fonctions irréductibles. Il est bien entendu que c'est parmi elles, et parmi elles seulement, que nous choisirons le premier membre de notre équation réductrice.

Pour rendre les remarques ultérieures plus claires en les rapportant à un exemple, nous allons maintenant donner un fragment d'une Table de puissances toute construite; cela nous suffira amplement. Dans cet exemple, nous avons

$$m = 5, \qquad n = 3,$$

et l'équation réductrice est

$$x^3 + 4x + 2 = 0.$$

De même que précédemment pour les fonctions, nous écrirons conventionnellement les polynomes en i, sans écrire la lettre i elle-même; ainsi, i s'écrira 10, 431 signifiera $4i^2 + 3i + 1$, ...

Fig. 34.

k	i^k	k	i^k	k	i^k	k	i^k	k	i^k
1	010	8	043	15	311	22	331	29	312
2	100	9	430	16	144	23	344	30	104
3	013	10	342	17	403	24	424	31	003
4	130	11	404	18	022	25	232		
5	313	12	032	19	220	26	341		
6	114	13	320	20	221	27	444		
7	103	14	234	21	231	28	432		

Comme on le voit, cette Table a pour base une racine de l'équation $x^3 + 4x + 2 = 0$, ce qui nous donne

$$i^3 = -4i - 2 = i + 3.$$

Les calculs des puissances successives se font très rapidement, en multipliant toujours par i et remplaçant i^3, chaque fois qu'il apparaît, par la fonction réductrice $i+3$.

Le module des indices est

$$5^3 - 1 = 124 = 2^2.31.$$

La figure ne comprend donc que le quart de la Table complète; mais cela nous suffit pour reconnaître que la fonction réductrice choisie est bien à racines primitives, et aussi pour pouvoir achever la Table, si nous le voulions, pour ainsi dire sans calcul.

Nous tombons, en effet, sur $i^{31} = 3$; de là

$$i^{62} = 4, \qquad i^{93} = 2, \qquad i^{124} = 1.$$

Il est donc certain que la Table sera complète, qu'elle aura 124 termes tous différents. Maintenant, les 31 premiers étant calculés dans le Tableau ci-dessus, soit k l'indice d'un terme quelconque. Le mécanisme même du calcul nous montre que, pour avoir le terme d'indice $31 + k$, il n'y aura qu'à multiplier i^k par 3, c'est-à-dire qu'on aura le deuxième quart de la Table, en multiplant par 3 tous les termes du premier quart; de même, en multipliant par 4, puis par 2, ces mêmes termes, on obtiendra le troisième et le quatrième quarts.

Dans cet exemple, on est donc bien parti d'une fonction réductrice à racines primitives. Pour la trouver, le module des indices étant en général décomposé en facteurs premiers sous la forme $a^\alpha b^\beta\ldots$ (ici 2^2, 31), voici le procédé qu'indique Galois : il remarque qu'il suffit d'obtenir une racine primitive de chaque équation

$$x^{a^\alpha} = 1, \qquad x^{b^\beta} = 1, \qquad \ldots.$$

C'est dans cette recherche que le tâtonnement intervient. Une fois cette détermination faite, il n'y aura plus qu'à multiplier entre elles les fonctions obtenues, pour avoir une racine primitive de l'équation $x^{m^n-1} - 1 = 0$. Le reste va de soi.

A ce procédé, en dehors des remarques faites plus haut sur l'exemple de la figure 34, on peut encore en ajouter d'autres. Par exemple, le dernier terme a_0 de la fonction réductrice devra être tel que $\pm a_0$ soit une racine primitive par rapport au module m;

il faut prendre le signe + si n est pair et — si n est impair. Cela donne un précieux élément d'exclusion, et cela s'établit très simplement. En effet, si i, i^m, i^{m^2}, ..., $i^{m^{n-1}}$ sont les racines de l'équation, leur produit sera

$$i^{1+m+\ldots+m^{n-1}} = i^{\frac{m^n-1}{m-1}}.$$

Élevé à ses puissances successives, il ne devra jamais donner 1 que lorsqu'on sera arrivé à sa puissance de degré $m-1$. Or ce produit, qui est un entier, est précisément $\pm a_0$, et la propriété indiquée est celle qui caractérise une racine primitive (module m).

59. Nous avons dit plus haut comment on pourrait, en regard de chaque imaginaire de la Table, obtenir l'équation dont cette imaginaire est racine, ou, ce qui revient au même, la case de l'espace représentatif où elle se logera. On peut en faire application ici, à l'indice 1 par exemple. Les deux autres racines sont i^5 et i^{25}. En regard des trois indices 1, 5, 25 nous avons 010, 313, 232 dont la somme est 0; en faisant les sommes 2 à 2 des indices nous avons 6, 26, 30, auxquels correspondent 114, 341, 104 dont la somme est 4; enfin la somme 31 des indices correspond à 3. Donc $x^3 + 4x - 3$, ou $x^3 + 4x + 2$ est le premier membre de l'équation réductrice; 1042 sera la notation de la case qui représente cette équation.

Voici maintenant une petite remarque qui abrégera beaucoup le calcul des cases pour les autres quarts de la Table. Lorsqu'on multiplie une imaginaire par un nombre k, les fonctions $\sigma_1, \sigma_2, \sigma_3, \ldots$ seront respectivement multipliées par k, k^2, k^3, ...

Donc, la case 1042 répondant à l'indice 1 et à l'imaginaire 10, les chiffres de la case qui répond à l'indice 32 seront obtenus en multipliant respectivement 1, 0, 4, 2 par 3, 3^2, 3^3, 3^4, ou 3, 4, 2, 1, puisque l'imaginaire d'indice 32 est

$$30 = 10 \times 3.$$

La case d'indice 32 aura donc pour chiffres

$$1 \times 3 = 3,\ 0 \times 4 = 0,\ 4 \times 2 = 3,\ 2 \times 1 = 2;$$

l'équation sera donc 3032, ou, en multipliant par 2, 1014.

Changement de base.

60. Ayant construit une Table, complète ou non, de puissances d'imaginaires, on peut être conduit à en former une autre, en prenant pour base l'un des termes de la première. Si, par exemple, on s'aperçoit que la première Table ne peut être complète, on sera parfois amené à un tel changement.

Il est alors intéressant de rechercher l'équation réductrice de la nouvelle Table, et il n'est pas besoin pour cela de connaître même celle de la première.

Appelons i la base de la première Table, $i^k = j$ le terme pris pour base de la seconde, et supposons qu'on en ait calculé les n premiers termes $j, j^2, j^3, \ldots, j^n$ exprimés chacun par un polynome en i de degré $n - 1$ au plus. Si entre ces n relations nous éliminons $i, i^2, \ldots, i^{n-1}$, il restera une relation en j de la forme $j^n + A_{n-1} j^{n-1} + \ldots + A_1 j + A_0 = 0$, qui sera l'équation réductrice de la nouvelle Table.

En supposant, par exemple, que $n = 4$, nous aurions

$$\begin{aligned} j &= a_3 i^3 + a_2 i^2 + a_1 i + a_0, \\ j^2 &= b_3 i^3 + b_2 i^2 + b_1 i + b_0, \\ j^3 &= c_3 i^3 + c_2 i^2 + c_1 i + c_0, \\ j^4 &= d_3 i^3 + d_2 i^2 + d_1 i + d_0. \end{aligned}$$

L'équation réductrice pourrait s'écrire sous la forme

$$\begin{vmatrix} j - a_0 & a_3 & a_2 & a_1 \\ j^2 - b_0 & b_3 & b_2 & b_1 \\ j^3 - c_0 & c_3 & c_2 & e_1 \\ j^4 - d_0 & d_3 & d_2 & d_1 \end{vmatrix} = 0,$$

ou

$$D(j^4 - d_0) + C(j^3 - c_0) + B(j^2 - b_0) + A(j - a_0) = 0,$$

en appelant A, B, C, D les déterminants mineurs pris avec les signes convenables.

Il est bon de remarquer que la connaissance de l'équation réductrice de la première Table est complètement inutile pour la

recherche que nous venons de faire. D'ailleurs, elle peut être obtenue sans beaucoup de peine. Supposons seulement la Table j poussée jusqu'à j^6 dans le cas de $n = 4$ qui vient de nous servir.

Écrivons les identités $j^2 = j^2, j^4 = j^4, j^6 = j^6$, en formant le premier membre de chacune au moyen de la fonction en i du troisième degré qui représente, soit j, soit j^2, soit j^3, et en remplaçant les j^2, j^4, j^6 par les fonctions de i lues dans la Table. Cela nous donnera trois équations de la forme

$$\alpha_6 i^6 + \alpha_5 i^5 + \alpha_4 i^4 + \ldots + \alpha_0 = 0,$$
$$\beta_6 i^6 + \ldots\ldots\ldots\ldots\ldots + \beta_0 = 0,$$
$$\gamma_6 i^6 + \ldots\ldots\ldots\ldots\ldots + \gamma_0 = 0.$$

L'élimination de i^6 et i^5 entre ces équations nous donnera l'équation réductrice en i.

Nous donnons (*fig.* 35) le quart d'une Table de puissances où l'on a pris pour base le polynome $i^3 + i^2 + 2$. On a dans cette figure

$$m = 5, \qquad n = 4, \qquad \mathfrak{M} = 624.$$

Il serait très facile de la prolonger, et le lecteur y pourra trouver matière à d'intéressants exercices.

Table de puissances des imaginaires du quatrième ordre, module 5.

Fig. 35.

IND.	IMAG.	IND.	IMAG.	IND.	IMAG.	IND.	IMAG.	IND.	IMAG.	IND.	IMAG.
1	1102	27	1041	53	4231	79	0444	105	3240	131	1213
2	4141	28	2300	54	2332	80	3214	106	0032	132	1432
3	3132	29	4001	55	4211	81	1424	107	0210	133	2213
4	1042	30	4432	56	0343	82	3440	108	1411	134	3102
5	3402	31	3323	57	2440	83	0421	109	4122	135	3031
6	3142	32	1011	58	3201	84	3424	110	2240	136	0223
7	2014	33	4344	59	2101	85	2330	111	3312	137	0234
8	4310	34	1322	60	0214	86	2012	112	4442	138	2303
9	4413	35	1024	61	0314	87	2111	113	4340	139	2302
10	2431	36	3112	62	0031	88	1231	114	2424	140	1200
11	3331	37	4003	63	4113	89	1222	115	0110	141	2114
12	0334	38	1131	64	2320	90	1302	116	1244	142	4032
13	2020	39	1000	65	1040	91	4030	117	0040	143	3040
14	1434	40	2220	66	1203	92	1341	118	4033	144	0143
15	4412	41	1323	67	0410	93	2411	119	4142	145	2001
16	1334	42	2121	68	1300	94	1342	120	4234	146	0042
17	4240	43	2203	69	2331	95	4013	121	0133	147	1232
18	2202	44	2130	70	3114	96	0433	122	1034	148	2324
19	1033	45	2123	71	1202	97	1140	123	4134	149	0443
20	3032	46	4402	72	4313	98	1420	124	0431	150	2112
21	1320	47	0312	73	2214	99	4042	125	2402	151	2333
22	4320	48	3332	74	4204	100	4012	126	1422	152	0313
23	0430	49	1431	75	2122	101	1001	127	1241	153	4434
24	3344	50	1111	76	3300	102	3322	128	2244	154	0022
25	4102	51	4011	77	1221	103	0414	129	2210	155	4243
26	0201	52	0404	78	0200	104	0203	130	0301	156	0003

Remarques sur les racines imaginaires.

61. Dans tous les développements qui précèdent, nous avons généralement supposé $m > n$, et nous avons fait remarquer, en ce qui concerne les solutions réelles, que, pour $n \geq m$, on peut toujours abaisser le degré de l'équation en appliquant le théorème de Fermat qui nous donne pour tout nombre entier $x^m = x$.

Dans la théorie des racines imaginaires, il n'en est plus ainsi, chaque équation de degré n devant avoir n racines. Mais toute cette théorie n'implique aucune hypothèse sur la grandeur de n, sous réserve des observations concernant l'emploi des dérivées (52), et elle convient à tous les cas, que n soit plus grand ou plus petit que m, ou qu'il lui soit égal. Il n'y a donc aucune autre restriction à faire, et cela tient à ce que les propriétés des indices n'ont rien à voir avec m, mais seulement avec $\mathfrak{M} = m^n - 1$, module des indices.

Quant au théorème de Fermat, il trouve son analogue dans la proposition en vertu de laquelle toute imaginaire d'ordre ν, ν étant un diviseur de n, est racine de l'équation binome $x^{m^\nu - 1} - 1 = 0$, ou $x^{m^\nu} = x$. Pour $\nu = 1$, c'est-à-dire pour les imaginaires du premier ordre, ou les entiers, cette équation devient $x^m = x$; c'est le théorème de Fermat, qui apparaît ici comme un simple cas particulier d'une proposition beaucoup plus générale.

Une autre observation assez intéressante est celle qui concerne les équations binomes dont les termes d'une Table complète de puissances sont les solutions. Prenons un terme quelconque i^k et proposons-nous, au moyen de la Table, d'extraire sa racine d'indice p, $\sqrt[p]{i^k} = i^{\frac{k}{p}}$. Il faut pour cela chercher sur la Table l'indice $\frac{k}{p}$ et prendre le terme correspondant, qui sera la racine cherchée. Si ce quotient $\frac{k}{p}$ est un nombre entier unique, c'est-à-dire si p est premier avec $\mathfrak{M}$, module des indices, nous aurons un terme unique. Si p n'est pas premier avec $\mathfrak{M}$, et si le plus grand codiviseur est D, il y aura indétermination partielle ou impossibilité, suivant que le numérateur k aura ou n'aura pas de facteurs communs avec $\mathfrak{M}$; et, en cas d'indétermination partielle, le nombre des

racines trouvées sera D. Enfin, si p est un diviseur de $\mathfrak{M}$, il y aura indétermination totale, c'est-à-dire p racines, ou bien impossibilité, suivant que k sera ou ne sera pas lui-même multiple de p.

Nous voyons ainsi que l'équation binome $x^p - i^k = 0$ trouve sur la Table des puissances une solution, plusieurs ou aucune. Il pourrait paraître singulier que cette équation n'ait pas p racines, étant de degré p. Mais il faut bien remarquer que notre Table ne contient que des imaginaires d'ordre n et d'ordres ν diviseurs de n. Nous constatons donc simplement que les autres racines sont des imaginaires d'autres ordres que ceux-là. L'équation binome dont il est question peut s'écrire $x^p - \varphi(i) = 0$, $\varphi(i)$ étant un polynome de degré inférieur à n.

Une fois de plus, nous voyons la division par ses symboles $\frac{k}{0}$, $\frac{0}{0}$, pareils à ceux de l'Algèbre, nous apporter des solutions imaginaires ou nous révéler l'indétermination. Seulement, la division arithmétique nous montre qu'il y a des degrés dans cette indétermination, et nous permet en quelque sorte de la mesurer, ce que ne saurait faire l'Algèbre.

62. Il est facile de reconnaître qu'une équation binome ne peut jamais servir d'équation réductrice pour former une Table complète de puissances d'imaginaires. En supposant $n = 4$, soit par exemple $x^4 - a = 0$ l'équation binome choisie. Les termes successifs de la Table, résultant de la relation $i^4 = a$, s'écriront

$$\begin{matrix} 0010 & 0100 & 1000 & 000a \\ 00a0 & 0a00 & a000 & 000a^2 & \ldots \end{matrix}$$

Si a est une racine primitive du module, on aura donc $4(m-1)$ et en général $n(m-1)$ résultats différents, et pas un de plus, au lieu de $m^n - 1$. Si a n'était pas racine primitive, on en aurait moins encore.

Construction d'une Table de puissances d'imaginaires par une division.

63. Les observations présentées au Chapitre IV sur l'analogie des Tables de puissances avec certaines divisions, rapprochées de

ce qui précède sur la construction de ces Tables, conduisent à un mode de construction rapide, uniforme, et tout à fait élémentaire. Il suffira en effet de diviser l'unité par le premier membre de l'équation réductrice, en ajoutant constamment des zéros à la droite du dividende, autant qu'il en faudra ; cette opération sera identique à celle qui a pour objet la conversion d'une fraction $\frac{1}{p}$ en décimales, en Arithmétique, à cette différence près que ce sera une division congruente. Les restes successifs, en commençant par 10, 100, ..., seront précisément les termes de la Table de puissances que nous voulons construire. Pour le reconnaître, il suffit de constater que les opérations sont exactement les mêmes que celles expliquées précédemment. Pour rendre ceci manifeste, nous allons, par ce procédé, reprendre la construction de la Table donnée figure 34. Ici $m = 5$, $n = 3$, et l'équation réductrice est $x^3 + 4x + 2 = 0$, dont le premier membre s'écrit symboliquement 1042.

```
1000         | 1042
 1300        |-------------------------------
  3130       | 10131104340323140222334234431
   1140
    1030
     04300
       3420
        4040
         03200
           2340
            3110
             1440
              4030
               02200
                 2210
                  2310
                   3310
                    3440
                     4240
                       2320
                        3410
                         4440
                          4320
                           3120
                            1040
                             003
```

Dans une telle division, si $f(x)$ est le diviseur, on a l'iden-

tité

$$x^k = f(x)\, q_k(x) + R_k(x),$$

q_k étant le quotient, et, par suite, si i est une racine de $f(x) = 0$,

$$i^k = R_k(i).$$

Si l'on a pris un diviseur $f(x)$ quelconque, il est aisé de constater les résultats suivants :

La suite des opérations est toujours périodique ;

Pour qu'elle soit périodique mixte, il faut que l'équation $f(x) = 0$ ait au moins une racine nulle ;

Si $f(x) = 0$ a une racine multiple, le nombre des termes de la période, p, est congru au module m.

Tout cela est très facile à établir, et à vérifier sur des exemples. Il pourrait y avoir encore bien des remarques intéressantes à faire sur ces questions; mais nous tenons à abréger, et nous bornons à ce qui est le plus essentiel.

Observations sur le cas du module 2.

64. Dans tout ce qui précède, nous avons en principe considéré toujours un module premier, mais en fait nos applications n'ont porté que sur des modules premiers impairs, 2 étant toujours laissé de côté. Cependant, il y a un avantage évident, lorsqu'on expose une théorie générale, à s'assurer qu'elle ne comporte pas d'exception, ou bien à approfondir, en les discutant, les causes des cas exceptionnels. C'est ce qui nous détermine à présenter ici quelques considérations rapides sur ce cas du module 2.

Tout d'abord, l'hypothèse $n < m$ devra être écartée, sans quoi la théorie ne pourrait s'appliquer qu'au premier degré, et perdrait presque tout intérêt. De ce seul fait résulteront les précautions à prendre qui ont été signalées précédemment, en particulier dans l'emploi des dérivées.

En second lieu, les représentations symboliques indiquées n'exigeront que l'emploi des deux caractères 0 et 1 de la numération binaire, ce qui sera seulement une simplification dans les écritures et les calculs.

Enfin, dans les puissances d'imaginaires, le module des indices $m^n - 1$, devenant $2^n - 1$, sera toujours impair, et pourra même être premier.

Sauf ces réserves, les principes généraux subsisteront, et trouveront leur application.

Ce qui caractérise essentiellement les équations et relations quelconques du module 2, c'est que les signes + et — se confondent, peuvent être changés l'un en l'autre à volonté, de telle sorte que l'emploi du signe — devient sans objet. Ceci résulte de ce que $A = -A$, puisque $2A = 0$ est ici une identité.

La représentation des fonctions de degré n se fera dans un espace à n dimensions, de module 2, dans lequel le numéro de chaque case se trouvera désigné par un symbole en numération binaire. Les coordonnées sur chaque axe ne pourront être que 0 ou 1.

Le classement des fonctions en réductibles et irréductibles se fera suivant les principes indiqués. Prenons par exemple $n = 3$. Il y aura huit équations $x^3 + cx^2 + bx + a = 0$, et huit seulement; nous en donnons ci-dessous le Tableau, avec l'indication de leurs racines réelles :

c.	*b.*	*a.*	Racines.
0	0	0	0, 0, 0
0	0	1	1
0	1	0	0
0	1	1	
1	0	0	0, 0, 1
1	0	1	
1	1	0	0
1	1	1	1

Il nous reste deux fonctions irréductibles

$$x^3 + x + 1, \quad x^3 + x^2 + 1.$$

Cherchons à former une Table de puissances d'imaginaires avec $i^3 + i + 1 = 0$, par exemple, comme équation réductrice, on trouve qu'elle sera

$i.$	$i^2.$	$i^3.$	$i^4.$	$i^5.$	$i^6.$	$i^7.$
10	100	11	110	111	101	1



C'est une Table complète, car le module des indices est

$$2^3 - 1 = 7.$$

La seconde équation irréductible

$$x^3 + x^2 + 1 = 0$$

serait aussi à racines primitives.

Pour le quatrième degré, on a trois fonctions irréductibles

$$x^4 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1.$$

Le module des indices est 15; les deux premières fonctions sont à racines primitives, et la troisième ne l'est pas; elle a pour gaussien 5.

Pour le cinquième degré, le module des indices est 31; il y a six fonctions irréductibles, toutes à racines primitives, et qu'on peut écrire

100101, 101001, 101111, 110111, 111011, 111101.

Les groupements des indices, par équations, sont

(1, 2, 4, 8, 16) (3, 6, 12, 24, 17) (5, 10, 20, 9, 18)
(7, 14, 28, 25, 19) (11, 22, 13, 26, 21) (15, 30, 29, 27, 23)

Nous laissons au lecteur le soin de vérifier ces résultats, et de faire d'autres applications.



CHAPITRE VII.

VARIATIONS DES FONCTIONS ARITHMÉTIQUES.

Rappel de formules algébriques.

65. Dans tout ce qui précède, nous nous sommes spécialement attaché à l'étude des équations arithmétiques, en employant, comme on l'a vu, une méthode essentiellement synthétique. Nous avons classé toutes les équations possibles d'un degré n déterminé, en montrant comment on peut construire aussi les racines, réelles ou imaginaires, de chacune d'elles, par rapport à un module premier m.

Une autre question, fort différente, va faire l'objet du présent Chapitre et sera examinée analytiquement. C'est celle qui consiste, étant donnée une fonction $f(x)$, non plus à chercher les valeurs de x qui la rendent nulle, mais à se rendre compte des valeurs successives que prendra $f(x)$ quand on donnera successivement à x toutes les valeurs possibles. Ici encore, ces valeurs de x seront en nombre limité m; et il y aura par suite m valeurs, distinctes ou non, de $f(x)$, puisque cette fonction est un polynome de degré n, qui prend une valeur, et une seule, quand x est déterminé. Nous supposerons constamment que n est inférieur à m.

On connaît les formules classiques de l'algèbre qui se rapportent à ces polynomes entiers et qui toutes sont finies, car elles ne prennent la forme de séries que pour des fonctions autres que des polynomes. C'est d'abord la formule de Taylor,

$$f(x+h) = f(x) + hf'(x) + \frac{h^2}{2!}f''(x) + \ldots + \frac{h^n}{n!}f^{(n)}(x).$$

qui donne en particulier, lorsqu'on y fait $h = 1$,

$$f(x+1) = f(x) + f'(x) + \frac{1}{2!}f''(x) + \ldots + \frac{1}{n!}f^{(n)}(x).$$

La formule de Maclaurin

$$f(x) = f(0) + xf'(0) + \frac{x^2}{2!}f''(0) + \ldots + \frac{x^n}{n!}f^{(n)}(0)$$

s'en déduit immédiatement.

La théorie des différences fait, en outre, connaître que, pour des valeurs de x en progression arithmétique de raison h, les fonctions $\Delta f(x)$, $\Delta^2 f(x)$, $\ldots$, $\Delta^n f(x)$ sont de degrés $n-1$, $n-2$, $\ldots$, 0, et

$$\Delta f(x) = h\; f'(x) + \frac{h^2}{2!}f''(x) + \ldots + \frac{h^n}{n!}f^{(n)}(x),$$
$$\Delta^2 f(x) = h\Delta f'(x) + \ldots + \frac{h^{n-1}}{(n-1)!}\Delta f^{(n-1)}(x),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Le problème de l'interpolation peut se résoudre, en ce qui concerne les polynomes, par les formules classiques de Lagrange ou de Newton, quand on connaît $n+1$ valeurs correspondantes de x et de $f(x)$ et, en particulier, lorsque les valeurs connues de x sont en progression par différence.

Signalons encore une forme moins employée mais souvent très commode, qui consiste, si α, β, γ, $\ldots$, λ sont les valeurs connues de la variable x, à écrire

$$\begin{aligned} f(x) = {} & A + B(x-\alpha) \\ & + C(x-\alpha)(x-\beta) + \ldots + M(x-\alpha)(x-\beta)\ldots(x-\lambda). \end{aligned}$$

On a alors le système d'équations

$$\begin{aligned} & A = f(\alpha), \\ & A + B(\beta-\alpha) = f(\beta), \\ & A + B(\beta-\alpha) + C(\gamma-\alpha)(\gamma-\beta) = f(\gamma), \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{aligned}$$

qui permet de déterminer de proche en proche tous les coefficients A, B, C, $\ldots$, M, au nombre de $n+1$.

Toutes ces relations sont invariablement applicables lorsqu'on

les considère comme des équations arithmétiques avec un module premier, car les expressions fractionnaires qu'elles présentent se transforment en nombres entiers, les dénominateurs ne pouvant jamais contenir en facteur le module. C'est pour cette raison que nous avons supposé $n < m$.

Comme conséquence de la formule de Maclaurin, il est bon de remarquer que si l'on a

$$f(x) = a_n x^n + \ldots + a_p x^p + \ldots + a_1 x + a_0,$$

on a aussi, identiquement,

$$f(0) = 0, \quad f'(0) = a_1, \quad \ldots, \quad f^{(p)}(0) = a_p p!, \quad \ldots, \quad f^{(n)}(0) = n! a_n.$$

Représentation graphique d'une fonction.

66. Lorsqu'on veut représenter, en Géométrie analytique, les variations d'une fonction $f(x)$, polynome entier de degré n, on le fait par une courbe, dont l'équation $y = f(x)$ est celle d'une parabole du $n^{\text{ième}}$ ordre. Cette courbe est entièrement déterminée dès que $n+1$ de ses points sont connus.

De même, ici, nous pourrons déterminer entièrement les m points ayant pour ordonnées $f(0)$, $f(1)$, ..., $f(m-1)$ et pour abscisses 0, 1, ..., $m-1$, dans un espace arithmétique à deux dimensions de module m, et joindre successivement ces points par des lignes droites, cela nous donnera des traits en ligne brisée que nous pourrons appeler des *paraboles arithmétiques d'ordre n et de module m*. Il existe évidemment m^n de ces paraboles, si l'on y comprend celles d'ordres inférieurs et seulement

$$(m-1)m^{n-1} = m^n - m^{n-1},$$

si l'on ne considère que celles qui sont effectivement d'ordre n; cela veut dire que, dans la fonction $f(x)$, on suppose différent de zéro le coefficient de x^n.

Chacune de ces paraboles peut être entièrement déterminée, quand on connaît $n+1$ de ses points; cela permet de trouver tous les autres. Ceci est une extension de la détermination d'une ligne droite par deux de ses points.



Avant d'aller plus loin, élucidons ceci par un exemple, dans l'hypothèse $m = 7$, $n = 4$, en considérant la fonction

$$f(x) = x^4 + 3x^3 + x^2 + 2x + 5.$$

Pour

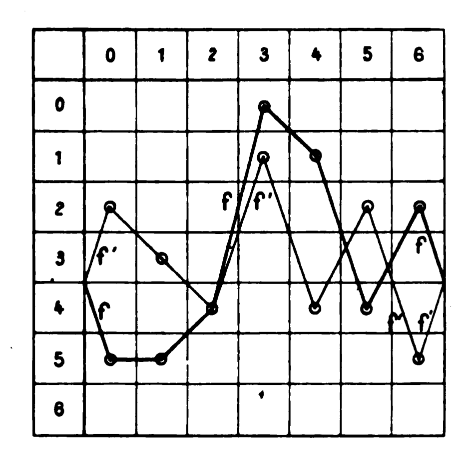
x	0	1	2	3	4	5	6

on a

$f(x) = y$	5	5	4	0	1	4	2

La parabole correspondante, du quatrième ordre, sera donc représentée par la figure ci-dessous :

Fig. 36.



En traits plus faibles, nous avons figuré la représentation de la dérivée

$$f'(x) = 4x^3 + 2x^2 + 2x + 2.$$

Nous engageons le lecteur à construire des figures représentatives analogues, parmi lesquelles nous indiquons spécialement celles qui correspondent à la fonction

$$f(x) = x^4 + 6x^3 + 3x^2 + 3x + 2$$

et à ses dérivées. Le fait assez remarquable d'une racine commune ($x = 2$) à l'équation $f(x) = 0$ et à toutes ses dérivées montre que la fonction $f(x)$ est identique à $(x - 2)^4$ par rapport au module 7.

Différences successives.

67. Sur la figure du numéro précédent, nous pouvons facilement vérifier les propriétés des différences, rappelées plus haut. Il suffit, pour cela, de former le Tableau :

f......	5	5	4	0	1	4	2
Δf.....	0	6	3	1	3	5	
$\Delta^2 f$.....	6	4	5	2	2		
$\Delta^3 f$.....	5	1	4	0			
$\Delta^4 f$.....	3	3	3				

Les mêmes Tableaux, pour les dérivées successives

$$f'(x) = 4x^3 + 2x^2 + 2x + 2,$$
$$f''(x) = 5x^2 + 4x + 2,$$
$$f'''(x) = 3x + 4,$$

sont

f'......	2	3	4	1	4	2	5
$\Delta f'$....	1	1	4	3	5	3	
$\Delta^2 f'$....	0	3	6	2	5		
$\Delta^3 f'$....	3	3	3	3			
f''......	2	4	2	3	0	0	3
$\Delta f''$....	2	5	1	4	0	3	
$\Delta^3 f''$....	3	3	3	3	3		
f'''.....	4	0	3	6	2	5	1
$\Delta f'''$....	3	3	3	3	3	3	

Analogies géométriques.

68. Il est bon de remarquer que les tracés en lignes brisées indiqués ci-dessus ne répondent à aucune réalité géométrique et sont purement conventionnels. Il faudrait plutôt imaginer que la courbe ayant pour équation $y = f(x)$ a été effectivement construite, et que, la sectionnant dans les divers carrés de module m, on en a reproduit les sections dans le carré de module m, qui fournit ainsi l'image de tous les points à coordonnées entières, comme cela a

lieu pour les droites. Mais, cette observation faite, il reste des analogies intéressantes que nous nous bornerons seulement à indiquer, et qu'il serait facile de pousser beaucoup plus loin que nous ne le ferons ici.

Par exemple, α et $\beta = f(\alpha)$ étant les deux coordonnées d'un point d'une de nos paraboles (ou de la case qui a ce point pour centre), soit β' la valeur correspondante de la dérivée $f'(\alpha)$. Si, partant du point α, β, nous marchons du pas $1.x + \beta'.y$, nous obtiendrons tous les points d'une droite qui sera la tangente à la courbe au point considéré. On aura ainsi

$$\begin{array}{l}(\alpha,\ \beta),\\ (\alpha+1,\ \beta+\ \beta'),\\ (\alpha+2,\ \beta+2\beta'),\\ \dots\dots\dots\dots\dots,\\ {[\alpha+m-1,\ \beta+(m-1)\beta']}.\end{array}$$

De même, les points de la normale seront donnés par la marche, perpendiculaire à la précédente,

$$\beta'.x - 1.y.$$

en sorte que ses points ont pour coordonnées

$$(\alpha,\ \beta),\quad (\alpha+\beta',\ \beta-1),\quad \dots,\quad [\alpha+(m-1)\beta',\ \beta+(m-1)]$$ [1].

Une autre remarque utile, c'est que les transformations de coordonnées ayant pour objet le transport parallèle des axes sont intégralement applicables; le seul effet qu'elles produisent est de déplacer tout d'une pièce le diagramme qui représente conventionnellement une parabole quelconque. Ainsi les paraboles

$$y = f(x), \qquad y + k = f(x + h)$$

seront telles que l'une s'obtiendra immédiatement dès qu'on connaîtra l'autre; il suffira de partir de la case ayant pour coordonnées h, k, au lieu de la case origine o, o.

---

[1] On peut dire aussi que la tangente et la normale ont respectivement pour équations

$$y = \beta' x + \beta - \alpha\beta',$$
$$y = -\frac{1}{\beta'}x + \beta + \frac{\alpha}{\beta'}.$$

Soient M un point (α, β), MTT′ la tangente et MNN′ la normale coupant l'axe des x en T et N, l'axe des y en T′ et N′, respectivement, et MP, MQ l'ordonnée et l'abscisse de M. Si nous appelons PT, PN la sous-tangente et la sous-normale par rapport à Ox; QT′, QN′ la sous-tangente et la sous-normale par rapport à Oy, les équations de la tangente et de la normale montrent que les sous-tangentes auront pour expressions

$$-\frac{\beta}{\beta'} \text{ par rapport à } Ox,$$

$$-\alpha\beta' \text{ par rapport à } Oy,$$

et les sous-normales

$$\beta\beta' \text{ par rapport à } Ox,$$

$$\frac{\alpha}{\beta'} \text{ par rapport à } Oy.$$

Comme simple exemple relatif à ces analogies, prenons une parabole du deuxième ordre (module 7). La remarque sur la transformation des coordonnées, présentée ci-dessus, nous montre qu'on peut toujours, par un simple transport, ramener l'équation à la forme $y = Ax^2$; alors le sommet est à l'origine, et l'axe de la courbe est Oy. Supposons $A = 3$. En donnant à x toutes les valeurs possibles, nous avons le Tableau suivant :

α.....	0	1	2	3	4	5	6
β.....	0	3	5	6	6	5	3
β'....	0	6	5	4	3	2	1

On vérifie que

$$\frac{\alpha}{\beta'} = \text{const.} = 6$$

et que

$$-\alpha\beta' = -2\beta.$$

Ainsi, dans nos paraboles arithmétiques, nous retrouvons ces propriétés bien connues, que la sous-normale est constante, et que la sous-tangente, changée de signe d'après notre convention, est double de l'ordonnée.

Interpolation.

69. Nous allons dire maintenant quelques mots du problème inverse, consistant à déterminer une fonction de degré n, ou une parabole d'ordre n, connaissant $n+1$ points de cette dernière, c'est-à-dire $n+1$ couples de valeurs correspondantes de x et de y.

Tout d'abord, si les valeurs données de x sont en progression par différence, la théorie des différences nous fournira une solution très rapide, en nous rappelant que les différences $n^{\text{ièmes}}$ sont constantes. Soit, par exemple, $m = 7$, $n = 4$ et, pour

x........	2	3	4	5	6
$f(x)$.....	2	5	3	2	6

Nous formerons le Tableau

2	5	3	2	6	3	0
3	5	6	4	4	4	2
2	1	5	0	0	5	1
6	4	2	0	5	3	1
5	5	5	5	5	5	5

Il s'ensuit que pour

x........	0	1	2	3	4	5	6
$f(x)$.....	3	0	2	5	3	2	6

Tous les points de la parabole sont connus et l'on trouve pour la fonction

$$f(x) = 4x^4 + x^3 + 3x^2 + 3x + 3,$$

résultat qu'aurait d'ailleurs fourni la formule d'interpolation de Newton.

Supposons maintenant qu'on donne $n+1$ points quelconques de la parabole à déterminer. Par exemple, toujours pour $m = 7$, $n = 4$, soit

x........	0	1	3	4	6
$f(x)$.....	4	1	5	1	2

Soit par la formule de Lagrange

$$f(x) = \frac{(x-1)(x-3)(x-4)(x-6)}{(-1)(-3)(-4)(-6)}4$$
$$+\frac{x(x-3)(x-4)(x-6)}{1(1-3)(1-4)(1-6)}1+\frac{x(x-1)(x-4)(x-6)}{3(3-1)(3-4)(3-6)}5$$
$$+\frac{x(x-1)(x-3)(x-6)}{4(4-1)(4-3)(4-6)}1+\frac{x(x-1)(x-3)(x-4)}{6(6-1)(6-3)(6-4)}2.$$

Soit en posant

$$f(x) = A + Bx + Cx(x-1) + Dx(x-1)(x-3)$$
$$+ Fx(x-1)(x-3)(x-4),$$

on obtiendra la fonction cherchée; dans le second cas, on remplacera successivement x par 0, 1, 3, 4, 6 et l'on aura successivement A, B, C, D, F.

Il peut être commode aussi de former le Tableau des différences, en remplaçant par des lettres les valeurs de $f(x)$ qui font défaut

4	1	α	5	1	β	2
4	$\alpha-1$	$5-\alpha$	3	$\beta-1$	$2-\beta$	
$\alpha+2$	$6-2\alpha$	$5+\alpha$	$\beta+3$	$3-2\beta$		
$4-3\alpha$	$6+3\alpha$	$5-\alpha+\beta$	-3β			
$2+6\alpha$	$6-4\alpha+\beta$	$2+\alpha-4\beta$				
$4-3\alpha+\beta$	$3+5\alpha-5\beta$					

En égalant à zéro les deux différences cinquièmes, on a

$$3\alpha-\beta=4, \qquad 5\alpha-5\beta=4,$$

et l'on tire de là facilement

$$\alpha=3, \qquad \beta=5.$$

Dès lors, on a toutes les valeurs de $f(x)$

4 1 3 5 1 5 2

et le problème, ramené au cas précédent, est entièrement résolu. La fonction cherchée est

$$2x^4+6x^2+3x+4.$$

Factorielles.

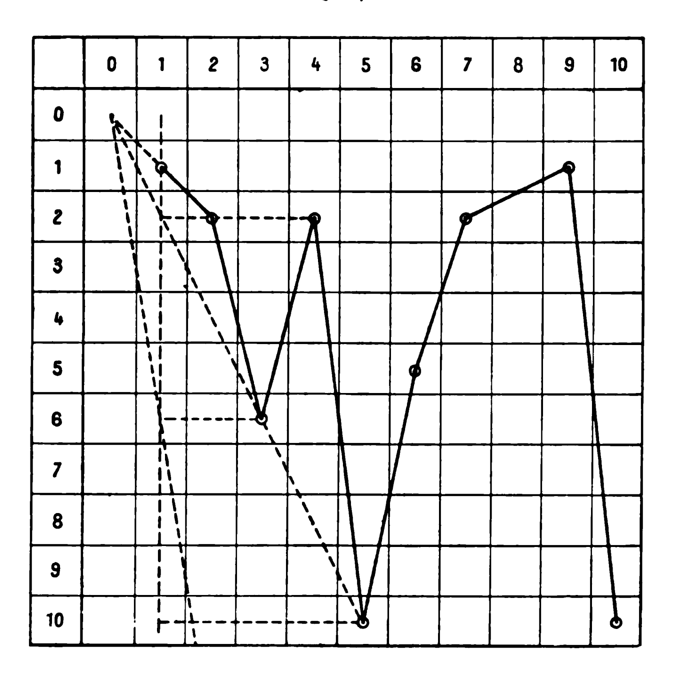
70. En principe, nous avons dit que nous nous occupions exclusivement dans cet Ouvrage des polynomes à coefficients entiers. Nous croyons ici devoir faire une exception à cette règle, pour dire quelques mots des fonctions appelées *factorielles,* qui jouent dans l'Arithmétique un rôle considérable.

Rappelons qu'on nomme *factorielle* d'un nombre entier x, et qu'on représente par $x!$ le produit $1.2.3...x$ de tous les nombres entiers consécutifs depuis l'unité jusqu'à x. Il peut être intéressant d'étudier, par rapport au module premier m, la fonction $x!$ et d'en représenter les variations comme il a été indiqué plus haut.

A l'inverse de ce que nous avons constaté jusqu'à présent, le champ de variation se limitera rigoureusement de 1 à m; car, pour $x \geqq m$, on aura constamment $x! = 0$. Au contraire, pour toute valeur de x inférieure à m, on n'aura jamais $x! = 0$, puisque m est premier. Le théorème de Wilson nous apprend, en outre, que, pour $x = m - 1$, la fonction deviendra $m - 1$, d'où il suit que, pour $x = m - 2$, nous aurons $x! = 1$.

Comme exemple, prenons $m = 11$:

Fig. 37.



Nous aurons le tracé de la figure 37, dans lequel se vérifient les propriétés indiquées ci-dessus. On remarquera que, pour passer d'une ordonnée y_{n-1}, correspondant à $x = n - 1$, à la suivante y_n, il suffit de former ny_{n-1}. Soit par le calcul, soit graphiquement comme l'indique la figure, cette opération peut se faire très simplement. Il suffit, en effet, de ramener l'ordonnée y_{n-1} dans la colonne d'abscisse 1, et de marcher de n pas sur la ligne caractérisée par $1.x + y_{n-1}.y$ à partir de la case origine. Autrement dit, on joindra le centre de la case origine à celui de la case dont les coordonnées sont $x = 1$, $y = y_{n-1}$ et l'on cherchera l'intersection de cette ligne avec celle qui a pour équation $x = n$.

En effectuant ces tracés, ou simplement ces calculs tout à fait faciles pour les plus petits nombres premiers, on obtient le Tableau suivant :

x \ m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
3	1	2																
5	1	2	1	4														
7	1	2	6	3	1	6												
11	1	2	6	2	10	5	2	5	1	10								
13	1	2	6	11	3	5	9	7	11	6	1	12						
17	1	2	6	7	1	6	8	13	15	14	1	12	3	8	1	16		
19	1	2	6	5	6	17	5	2	18	9	4	10	16	15	16	9	1	18

Ces Tables peuvent être très utiles pour évaluer, par rapport à un module premier m, un produit de plusieurs nombres consécutifs, le plus grand étant inférieur à m. Si par exemple nous considérons $5.6.7.8 \pmod{11}$, nous voyons que ce nombre peut s'écrire $\frac{8!}{4!}$ ou $\frac{5}{2}$, et la Table de division nous donne

$$\frac{5}{2} = 8.$$

On a donc

$$5.6.7.8 = 8.$$

Il est d'ailleurs évident que tout produit de facteurs entiers consécutifs en nombre inférieur à m, peut être ramené à cette forme, ou bien est nul. Ainsi

$$30.31.32.33.34 = 0$$

et

$$25.26.27.28.29 = 3.4.5.6.7 = \frac{7!}{2!} = \frac{2}{2} = 1.$$

71. On pourrait se proposer aussi d'étudier les factorielles par rapport à un module composé. Si nous considérons par exemple un produit $m = p.q$ de deux facteurs premiers ($p < q$), il est évident que les factorielles, jusqu'à $(p-1)!$ inclusivement, seront déterminées par rapport à m; depuis $(p-1)!$ jusqu'à $(q-1)!$ ce seront, par rapport à m, des multiples de p, qu'on pourra déterminer aussi. Enfin, à partir de $q!$ elles seront nulles indéfiniment.

Soit, par exemple,

$$m = 77 = 7.11.$$

Formons, d'après le Tableau précédent, les deux suites :

	1	2	3	4	5	6	7	8	9	10
7	1	2	6	3	1	6	0	0	0	0
11	1	2	6	2	10	5	2	5	1	10
77	1	2	6	24	43	27	35	49	56	21

Les valeurs cherchées, composant la dernière ligne, seront données par la Table de numération.

On peut, de même, étendre cette détermination des factorielles aux modules m composés du produit de plus de deux facteurs premiers, par un procédé complètement analogue. Ce sont toujours les Tables de numération qui permettront d'écrire les résultats sans avoir à faire aucun calcul.

Afin de ne laisser aucun doute dans l'esprit, nous croyons devoir, comme dernier exemple, donner ici le Tableau relatif au module

$$165 = 3.5.11.$$

	1	2	3	4	5	6	7	8	9	10
3	1	2	0	0	0	0	0	0	0	0
5	1	2	1	4	0	0	0	0	0	0
11	1	2	6	2	10	5	2	5	1	10
165	1	2	6	24	120	60	90	60	45	120

Il ne resterait plus qu'à étudier les factorielles par rapport à des modules de la forme a^α, a étant premier. Les Tableaux ci-dessous, relatifs à $m = 11^2$ et à $m = 7^3$, montrent que la question ne se pose que jusqu'à $(\alpha a)!$ exclusivement, et feront ressortir des propriétés simples sur lesquelles il nous semble inutile d'insister.

Module $121 = 11^2$	x....	1	2	3	4	5	6	7	8	9	10	11
	$x!$...	1	2	6	24	120	115	79	27	1	10	110
	x....	12	13	14	15	16	17	18	19	20	21	
	$x!$...	110	99	55	99	11	66	99	66	110	11	

	x	1	2	3	4	5	6	7
	$x!$	1	2	6	24	120	34	238
Module	x	8	9	10	11	12	13	14
$343 = 7^3$	$x!$	189	329	203	175	42	203	98
	x	15	16	17	18	19	20	
	$x!$	98	196	245	294	98	245	

Cercles arithmétiques.

72. Les considérations présentées au n° 68 montrent qu'on peut traduire aussi par des graphiques les variations de fonctions non entières. Comme simple exemple, nous pouvons considérer l'équation $x^2 + y^2 = r^2$, et construire les points, centres de cases ayant pour coordonnées les valeurs de x, y satisfaisant à cette équation. Par analogie, nous pourrons appeler ces figures des *cercles arithmétiques*.

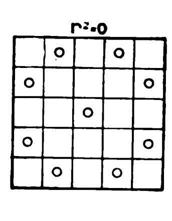
Pour présenter ces traductions graphiques sous une forme symétrique, nous supposerons l'origine transportée au centre de la case centrale du carré modulaire, case qui existe toujours, le module étant impair.

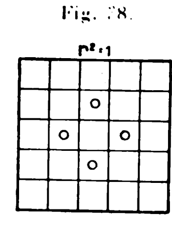
Les figures 38, 39, 40 sont assez faciles à comprendre, et à construire, pour dispenser de tout développement à ce sujet. Nous ferons seulement remarquer que le cercle pour lequel

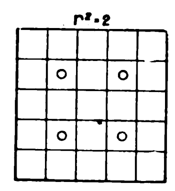
$$r^2 = 0 \qquad (\text{mod } 7)$$

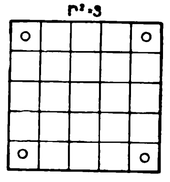
se réduirait à un point.

Fig. 38.









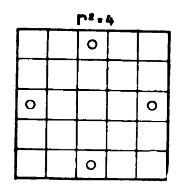


Fig. 39.

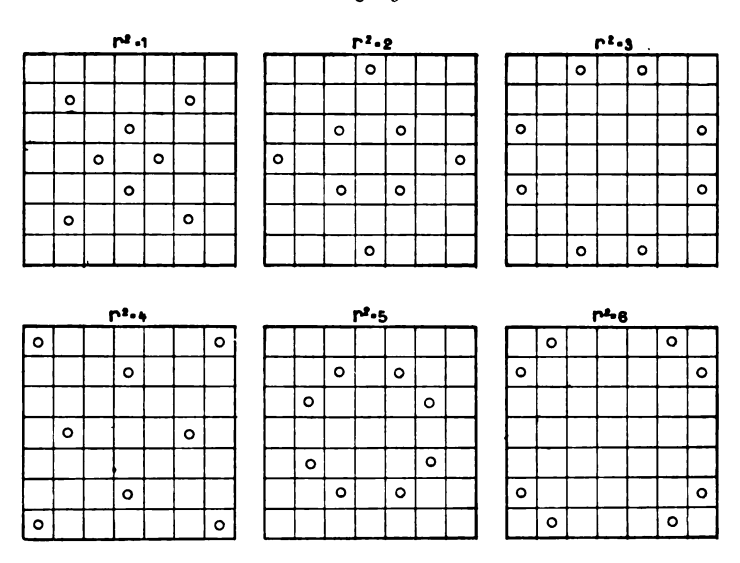
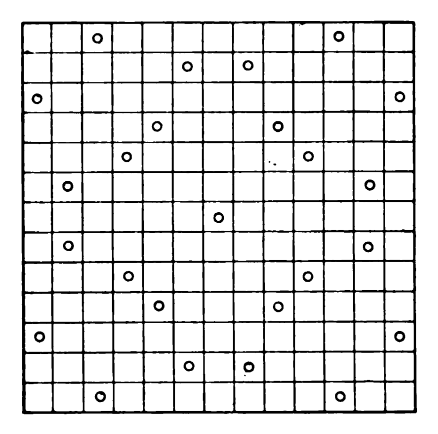


Fig. 40.



Si, au contraire, les cercles de rayon nul donnent des figures pour les modules 5 et 13, c'est que ces nombres sont des sommes de deux carrés. S'il n'en est pas ainsi, le cercle se réduit à son centre. Il est bon de remarquer que, lorsque r^2 n'est pas un carré, module m, on peut dire que le cercle est à rayon imaginaire.

Il serait aisé de construire de même des ellipses arithmétiques, d'équation

$$Ax^2 + By^2 = C,$$

des hyperboles équilatères

$$x^2 - y^2 = r^2,$$

des hyperboles quelconques

$$Ax^2 - By^2 = C.$$

Le lecteur pourra s'y exercer.

CHAPITRE VIII.

ÉTUDE DU PREMIER ET DU DEUXIÈME DEGRÉS.

Équations du premier degré.

73. Si, comme nous l'avons fait jusqu'à présent, on suppose que le coefficient du premier terme de chaque équation ait été ramené à 1, aucune question ne saurait se poser, l'équation étant résolue par cela même qu'elle est écrite. Mais, en considérant au contraire la forme générale $ax = b$, quelques observations peuvent trouver utilement place. D'abord, la résolution revient à déterminer le quotient $\frac{b}{a}$; et c'est parce que la division est toujours possible et uniforme, lorsque le module est premier, qu'une équation du premier degré a toujours une racine et une seule.

Si nous revenons pour un instant de l'équation modulaire à l'égalité arithmétique $ax = b + km$, nous voyons que, α étant racine de l'équation $ax = b$, le nombre $\alpha + \lambda m$ sera encore une racine, c'est-à-dire qu'il y en aura une infinité. Alors on aura les identités

$$a\alpha = b + km, \qquad a(\alpha + \lambda m) = b + (k + a\lambda)m.$$

Actuellement, considérons l'équation indéterminée à deux inconnues

$$lx + my = p,$$

et soient $l = Lm + a$, $p = Pm + b$, en supposant qu'on ait divisé l et p par m. Cette équation devient alors

$$(Lx + y - P)m + ax - b = 0.$$

Si nous y remplaçons x par $\alpha + \lambda m$, $ax - b$ devient

$$(k + a\lambda)m,$$

et nous avons

$$L(\alpha + \lambda m) + y - P + k + a\lambda = 0,$$
$$y = P - k - L\alpha - \lambda l.$$

Ainsi les valeurs $x = \alpha + \lambda m$, $y = P - k - L\alpha - \lambda l$ forment une solution de l'équation indéterminée $lx + my = p$. La résolution de l'équation modulaire du premier degré permet donc de résoudre les équations indéterminées à deux inconnues de la forme ci-dessus, lorsque le coefficient de l'une des inconnues est un nombre premier.

Naturellement, dans les formules qui précèdent, λ peut recevoir toutes les valeurs entières positives ou négatives; et k, qui peut être nul, s'obtient en calculant $\frac{a\alpha - b}{m}$.

Soit par exemple

$$32x + 7y = 54;$$

nous avons

$$32 = 4.7 + 4, \qquad 54 = 7.7 + 5;$$

l'équation modulaire $4x = 5$ nous donne la racine $\alpha = 3$; et

$$k = \frac{4.3 - 5}{7} = 1.$$

Les formules ci-dessus deviennent

$$x = 3 + 7\lambda, \qquad y = -(6 + 32\lambda),$$

et la vérification est immédiate.

74. Il est bon de remarquer aussi que les Tables de numération (**13**) résolvent au fond des questions du premier degré, et qu'elles donnent la solution du système indéterminé

$$ax + \alpha = by + \beta = cz + \gamma \ldots$$

lorsque a, b, c, ... sont premiers entre eux. En effet, on trouve dans la Table le nombre N, inférieur à $abc\ldots$, qui est égal à α

(module a), à β (module b), ... Il suffira donc d'écrire

$$x = \frac{N - \alpha}{a}, \qquad y = \frac{N - \beta}{b}, \qquad \ldots,$$

ou, plus généralement,

$$x = \frac{N' - \alpha}{a}, \qquad \ldots,$$

en posant

$$N' = N + \lambda abc\ldots.$$

Par exemple, soit le système

$$3x + 2 = 5y + 4 = 7z + 5.$$

La Table de numération nous donne

$$N = 89, \qquad N' = 89 + 105\lambda, \qquad x = \frac{89 - 2 + 105\lambda}{3} = 29 + 35\lambda$$

et

$$y = 17 + 21\lambda, \qquad z = 12 + 15\lambda.$$

D'ailleurs, l'équation

$$ax + \alpha = by + \beta$$

revient à

$$ax = \beta - \alpha \qquad (\bmod b),$$

en sorte que les Tables de numération pourraient, théoriquement, se construire en résolvant uniquement des équations du premier degré. Mais les procédés graphiques que nous avons indiqués sont incontestablement plus rapides.

Cas d'un module composé.

75. L'extrême simplicité qu'offre le premier degré permet de se rendre compte de ce que devient alors une équation dans le cas où le module est, non plus premier, mais composé. La résolution de l'équation $ax - b = 0$, revenant toujours à la détermination du quotient $\frac{b}{a}$, sera effectuée au moyen des Tables de division. L'équation pourra donc être impossible, avoir plusieurs racines ou

n'en avoir qu'une seule, comme nous l'avons déjà fait remarquer. Mais il est assez intéressant de constater que l'ensemble des équations ayant un même coefficient de x aura toujours en tout m racines différentes $0, 1, \ldots, m-1$. Ainsi (module 12) les équations

$$9x-1=0, \quad 9x-2=0, \quad 9x-4=0, \quad 9x-5=0,$$
$$9x-7=0, \quad 9x-8=0, \quad 9x-10=0, \quad 9x-11=0$$

n'ont pas de racines;

$$\begin{array}{lll} 9x=0 & \text{a pour racines} & 0, 4, 8, \\ 9x-3=0 & \text{»} & 3, 7, 11, \\ 9x-6=0 & \text{»} & 2, 6, 10, \\ 9x-9=0 & \text{»} & 1, 5, 9. \end{array}$$

On notera aussi, par exemple, que les racines de $8x-4=0$ sont

$$2, \quad 5, \quad 8, \quad 11$$

alors que $4x-2=0$ n'a aucune racine.

Ces remarques suffisent à montrer combien le cas des modules composés tend à éloigner des analogies entre les équations arithmétiques et celles de l'algèbre. Au fond, résoudre l'équation

$$ax+b=0,$$

si le module $m=pq$, p et q étant premiers entre eux, c'est la résoudre, *à la fois*, par rapport au module p et au module q. Si l'une des solutions est impossible, l'équation proposée ne pourra non plus être résolue. Si les solutions sont multiples, ou si l'une seulement présente ce caractère, il y aura plusieurs solutions, c'est-à-dire indétermination relative. Si enfin on a deux solutions uniques, la solution (module $m=pq$) sera unique aussi et fournie par une Table de numération.

Ces observations peuvent d'ailleurs s'étendre à une équation quelconque $f(x)=0$, même lorsque $f(x)$ n'est plus du premier degré.

Équation incomplète du deuxième degré.

76. Si $x^2 + bx + a = 0$ est une équation quelconque du deuxième degré, nous avons déjà vu qu'on peut en faire disparaître le deuxième terme. Il suffit pour cela de poser

$$z = x + \frac{b}{2},$$

d'où

$$x = z - \frac{b}{2},$$

si bien que l'équation proposée devient

$$z^2 - bz + \frac{b^2}{4} + bz - \frac{b^2}{2} + a = z^2 + a - \frac{b^2}{4} = 0.$$

Par conséquent, en prenant l'équation $x^2 + a = 0$, où le deuxième terme a disparu, nous ne particularisons pas, toute équation pouvant se ramener à celle-là.

Cette forme, dans le cas du deuxième degré qui nous occupe, a cela d'intéressant qu'elle permet la représentation par un espace à une dimension seulement, puisqu'on n'a plus qu'un seul coefficient a indéterminé.

Prenons, comme exemple très simple, $m = 7$, et formons la Table des puissances d'une racine primitive, 3, de 7 :

Indices..............	1	2	3	4	5	6
Puissances...........	3	2	6	4	5	1

Notre équation étant

$$x^2 + a = 0,$$

nous pouvons mettre x sous la forme

$$x = \sqrt[2]{-a}.$$

Pour que l'on ait des racines réelles, il faut donc que $-a$ soit un carré, c'est-à-dire que son indice soit pair; et il faudra, pour obtenir les racines, diviser l'indice par 2. Comme le module des

indices est $m - 1$, toujours divisible par 2, on a deux valeurs pour le quotient. Si I est l'indice de $-a$, les indices des deux racines seront $\frac{I}{2}$ et $\frac{I}{2} + \frac{m-1}{2}$.

Lorsque, au contraire, $-a$ a un indice impair, l'équation n'a pas de solutions réelles. On peut dire que ses racines sont imaginaires et les représenter quand même par le symbole $\sqrt{-a}$.

Par conséquent, pour $-a = 2, 4, 1$ ou $a = 5, 3, 6$, l'équation aura deux racines réelles, qui seront respectivement

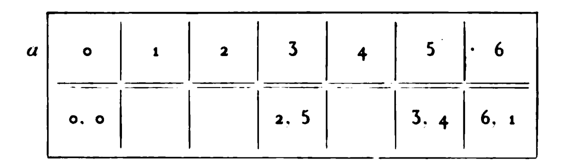
$$(3, 4)\quad (2, 5),\quad (6, 1).$$

Pour $-a = 3, 5, 6$ ou $a = 4, 2, 1$ les racines seront imaginaires et pourront être représentées par les symboles

$$\pm\sqrt[2]{3},\quad \pm\sqrt[2]{5},\quad \pm\sqrt[2]{6}.$$

Enfin, pour $a = 0$, on a une racine double, qui est nulle.

L'espace résolvant de l'équation $x^2 + a = 0$ sera donc



a	0	1	2	3	4	5	6
	0. 0			2. 5		3. 4	6. 1

Pour tout module premier, des circonstances analogues se présenteront évidemment.

Équation $x^2 + bx + a = 0$; solution algébrique.

77. Supposons maintenant que nous n'ayons pas fait disparaître le deuxième terme, et laissant à l'équation sa forme générale

$$x^2 + bx + a = 0,$$

que nous l'ayons résolue algébriquement, ce qui donne

$$x = -\frac{b}{2} \pm \sqrt{\frac{b^2}{4} - a}.$$

Cette formule nous donnera les racines, pour chaque équation, aussi bien qu'en Algèbre. Si $\frac{b^2}{4} - a$ est un carré, l'équation aura deux racines réelles; si cette expression n'est pas un carré, les racines seront imaginaires; enfin, si $\frac{b^2}{4} - a = 0$, les deux racines seront égales.

Dans la construction de l'espace résolvant, il est bien clair que les cases correspondant aux coordonnées b, a, telles que $\frac{b^2}{4} - a$ ne soit pas un carré, représentent des fonctions irréductibles. Cet espace à deux dimensions est très simple à construire. Nous le donnons ici (*fig.* 41) pour le cas de $m = 7$, déjà choisi plus haut.

Fig. 41.

b

a

	0	1	2	3	4	5	6
0	0,0			2,5		3,4	6,1
1	0,6	2,4	3,3			1,5	
2	0,5	6,6			1,4		2,3
3	0,4		5,6	1,3	2;2		
4	0,3		1,2	4,6	5;5		
5	0,2	1;1			3,6		4,5
6	0,1	3,5	4;4			2,6	

Nous avons noté que les équations à racines doubles sont celles pour lesquelles $\frac{b^2}{4} - a = 0$. Les cases correspondantes auront donc pour coordonnées celles d'un point de la parabole $y^2 - 4x = 0$ (*voir* Chap. VII). Ce sont ces cases que dans la figure nous avons signalées en entourant d'un cercle le couple des deux racines égales.

Application de la méthode de Galois.

78. Toutes les cases blanches de la figure 41 correspondent à des fonctions irréductibles. Nous pouvons partir de l'une quelconque d'entre elles pour former la Table des puissances d'imaginaires. Mais elle ne sera complète que si l'équation réductrice correspondante est à racines primitives. Cela ne peut avoir lieu, notamment, si l'équation réductrice choisie est binome. Mais les procédés de tâtonnement indiqués, et la méthode du changement de base, permettent assez facilement, surtout dans le cas simple du deuxième degré, d'arriver à fixer utilement le choix de cette équation réductrice. Nous prendrons ici l'équation

$$x^2 + 6x + 3 = 0,$$

d'où

$$i^2 = i + 4.$$

La division de 1000... par 163 (mod 7) nous donnera rapidement les $7^2 - 1 = 48$ puissances de i, formant la Table que nous cherchons. Dès le huitième reste, on reconnaîtra d'ailleurs si l'on est bien parti d'une équation réductrice à racines primitives. Ce reste, en effet, devra être une racine primitive du module 7, et c'est bien ce qui a lieu ici, puisque ce reste est 3.

Nous donnons ci-après (*fig.* 42, 43) la Table des puissances de i, et la Table inverse, c'est-à-dire celle qui présente, en regard de chaque fonction du premier degré, l'indice correspondant.

Puissances de i $(m = 7)$; **équation réductrice** $x^2 + 6x + 3 = 0$.

Fig. 42.

1	10	9	30	17	20	25	60	33	40	41	50
2	14	10	35	18	21	26	63	34	42	42	56
3	54	11	15	19	31	27	23	35	62	43	46
4	26	12	64	20	45	28	51	36	13	44	32
5	11	13	33	21	22	29	66	37	44	45	55
6	24	14	65	22	41	30	53	38	12	46	36
7	61	15	43	23	52	31	16	39	34	47	25
8	03	16	02	24	06	32	04	40	05	0 = 48	01



Indices correspondant aux fonctions de *i*.

Fig. 43.

01	0	23	27	45	20
02	16	24	6	46	43
03	8	25	47	50	41
04	32	26	4	51	28
05	40	30	9	52	23
06	24	31	19	53	30
10	1	32	44	54	3
11	5	33	13	55	45
12	38	34	39	56	42
13	46	35	10	60	25
14	2	36	46	61	7
15	11	40	33	62	35
16	31	41	22	63	26
20	17	42	34	64	12
21	18	43	15	65	14
22	21	44	37	66	29

Il est aisé, comme nous l'avons montré en général, de déterminer, pour chaque puissance de i, l'équation dont cette puissance est une racine; on arrive ainsi à grouper comme il suit les puissances de i (*fig.* 44) :

Fig. 44.

Indices des racines.	Équations.	Indices des racines.	Équations.
1,7	163	18,30	131
2,14	152	19,37	123
3,21	116	20,44	102
4,28	104	*24,24	121
5,35	145	25,31	113
6,42	141	26,38	122
*8,8	112	27,45	166
9,15	146	*32,32	162
10,22	114	33,39	136
11,29	135	34,46	164
12,36	101	*40,40	144
13,43	153	41,47	125
*16,16	134	*0,0	151
17,23	155		

Les astérisques indiquent les racines doubles, qui seules sont réelles.

Si nous dressons le Tableau inverse comprenant toutes les autres équations, irréductibles celles-là, avec les indices de leurs racines en regard, nous aurons la figure 45.

Fig. 45.

101	12,36	123	19,37	146	9,15
102	20,44	125	41,47	152	2,14
104	4,28	131	18,30	153	13,43
113	25,31	135	11,29	155	17,23
114	10,22	136	33,39	163	1,7
116	3,21	141	6,42	164	34,46
122	26,38	145	5,35	166	27,45

Enfin, il existe vingt-huit équations à racines réelles, dont nous donnons aussi le Tableau dans la figure 46 avec l'indication de leurs racines.

Fig. 46.

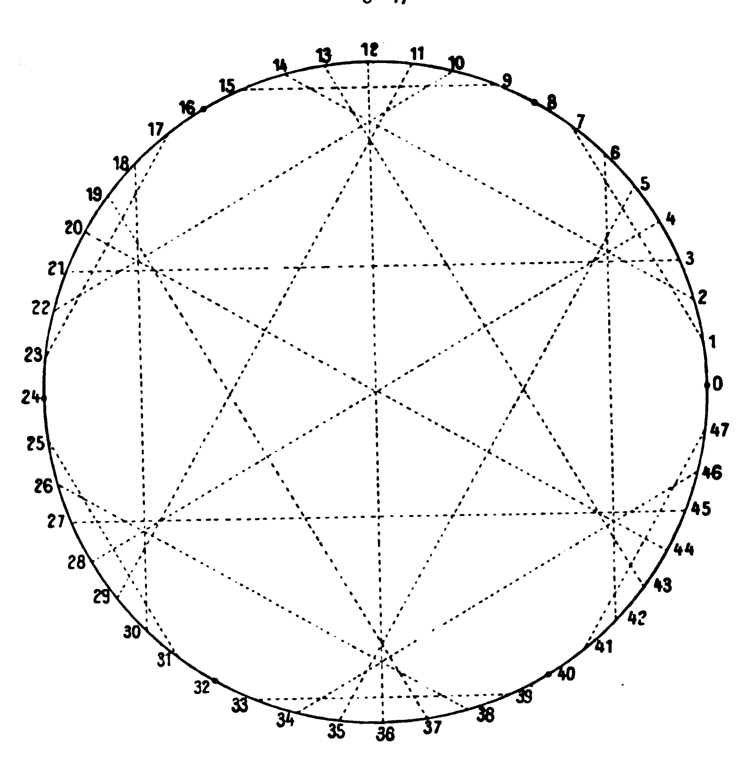
100	0,0	115	1,5	133	1,3	151	1,1
103	2,5	120	0,5	134	2,2	154	3,6
105	3,4	121	6,6	140	0,3	156	4,5
106	1,6	124	1,4	142	1,2	160	0,1
110	0,6	126	2,3	143	4,6	161	3,5
111	2,4	130	0,4	144	5,5	162	4,4
112	3,3	132	5,6	150	0,2	165	2,6

Nous avons ainsi la classification complète de toutes les équations du deuxième degré (module 7) avec leurs racines réelles ou imaginaires.

En ce qui touche les racines imaginaires, il est bon d'insister sur ce fait qu'on pourrait tout aussi bien prendre une autre base $j = i^k$, à la seule condition que k soit premier avec le module 48 des indices. A cette condition, la suite $1k$, $2k$, $3k$, ..., $48k$ reproduira en effet la suite complète 1, 2, ..., 48, dans un autre ordre.

Il nous semble intéressant, pour terminer ce Chapitre, de montrer ici (*fig.* 47) la représentation des puissances de i par la méthode géométrique qui est employée pour les imaginaires ordinaires de l'Algèbre. Les cordes en pointillé montrent comment se font les associations des deux racines i^k et i^{7k} d'une même équation. Les points noirs sur les divisions dont les indices sont multiples de 8 correspondent aux équations à racines réelles doubles.

Fig. 47.



Pour chaque équation figurée par l'une des cordes, joignant les points d'indices k et $7k$, il est aisé de la former assez simplement. Soit, en effet,

$$x^2 + b_k x + a_k = 0,$$

cette équation ayant pour racines i^k et i^{7k}. On a tout d'abord

$$a_k = i^{8k} = (i^8)^k = 3^k.$$

D'autre part, l'équation réductrice étant ici

$$x^2 + 6x + 3 = 0,$$

la fonction réductrice est $x + 4$, c'est-à-dire qu'on a

$$i^2 = i + 4.$$

Par suite, on a aussi

$$i^{14} = i^7 + 4.$$

Multipliant par i^k et par i^{7k} chacune de ces équations, il vient, respectivement,

$$i^{k+2} = i^{k+1} + 4\,i^k, \qquad i^{7(k+2)} = i^{7(k+1)} + 4\,i^{7k}.$$

De là, par addition,

$$i^{k+2} + i^{7(k+2)} = i^{k+1} + i^{7(k+1)} + 4(i^k + i^{7k}),$$

c'est-à-dire, en changeant les signes,

$$b_{k+2} = b_{k+1} + 4\,b_k.$$

Cette loi de récurrence est facile à vérifier sur les Tableaux numériques précédents. Elle permet de former de proche en proche les coefficients des deuxièmes termes des équations successives. On voit combien la formation des fonctions symétriques se simplifie dans le cas du deuxième degré.

CHAPITRE IX.

ÉTUDE DU TROISIÈME DEGRÉ.

Formule de Cardan; module $3n-1$.

79. L'équation générale du troisième degré est

$$x^3+cx^2+bx+a=0,$$

et elle peut se ramener à

$$x^3+bx+a=0,$$

forme non moins générale, à laquelle s'applique la formule de Cardan, au point de vue de la résolution algébrique.

Il y a une distinction importante à faire, suivant que le module m est de la forme $3n-1$ ou $3n+1$. C'est du premier cas que nous nous occuperons d'abord, en prenant $m=11$ comme exemple type.

Voici d'abord (*fig.* 48) le plan arithmétique donnant toutes les solutions réelles, pour $10ba$, correspondant à l'équation

$$x^3+bx+a=0.$$

Équation $x^3 + bx + a \equiv 0$, solutions réelles, module 11.

Fig. 48.

a \ b	0	1	2	3	4	5	6	7	8	9	10
0	∞ 0	10	4	2	6	8	3	5	9	7	1
1	0	2	7, 5 10	3					8	1, 4 6	9
2	3, 8 0	9		6, 6 10		4	7		5, 5 1		2
3	0	4		5, 8 9	10			1	2, 3 6		7
4	0		6	7		3, 9 10	1, 2 8		4	5	
5	0		3		2, 4 5	1	10	6, 7 9		8	
6	4, 7 0	8, 8 6	2		1			10		9	3, 3 5
7	2, 9 0			1	7, 7 8	5	6	4, 4 3	10		
8	5, 6 0		1, 1 9	4	3			8	7	10, 10 2	
9	0	1, 3 7			9	6	5	2			4, 8 10
10	1, 10 0	5	8			2, 2 7	9, 9 4			3	6

Passons maintenant à l'application de la formule de Cardan. Cette formule classique est

$$x = \sqrt[3]{-\frac{a}{2} + \sqrt[2]{R}} + \sqrt[3]{-\frac{a}{2} - \sqrt[2]{R}},$$

avec

$$R = \frac{a^2}{4} + \frac{b^3}{27}.$$

Représentons l'expression sous le premier radical cubique par A, et celle sous le second par B.

L'expression R ne contenant que des opérations directes, le résultat des calculs sera toujours un chiffre. Voici le Tableau des valeurs de R (*fig.* 49) correspondant à toutes les valeurs de a et de b :

Valeur de R, formule de Cardan, module 11.

Fig. 49.

b	$\frac{b^3}{27}$	0	1	2	3	4	5	6	7	8	9	10	a
			3	1	5	4	9	9	4	5	1	3	$\frac{a^2}{4}$
0	0	0	3	1	5	4	9	9	4	5	1	3	
1	9	9	1	10	3	2	7	7	2	3	10	1	
2	6	6	9	7	0	10	4	4	10	0	7	9	
3	1	1	4	2	6	5	10	10	5	6	2	4	
4	4	4	7	5	9	8	2	2	8	9	5	7	
5	3	3	6	4	8	7	1	1	7	8	4	6	
6	8	8	0	9	2	1	6	6	1	2	9	0	
7	7	7	10	8	1	0	5	5	0	1	8	10	
8	10	10	2	0	4	3	8	8	3	4	0	2	
9	5	5	8	6	10	9	3	3	9	10	6	8	
10	2	2	5	3	7	6	0	0	6	7	3	5	

Voici, en outre, la Table des puissances de la racine primitive 2, module 11 :

1	2	3	4	5	6	7	8	9	0	Indices.
2	4	8	5	10	9	7	3	6	1	Puissances.

Les puissances d'indice pair sont des carrés. Voici la Table de leurs racines :

1	3	4	5	9	carrés
1, 10	5, 6	2, 9	4, 7	3, 8	leurs $\sqrt[2]{\ }$

Considérons le cas où R est un carré. Nous donnons (*fig.* 50) le Tableau des racines carrées de R :

Valeur de $\sqrt[2]{\mathrm{R}}$, cas de R carré, module 11.

Fig. 50.

a \ b	0	1	2	3	4	5	6	7	8	9	10
0		5 6	1 10	4 7	2 9	3 8	3 8	2 9	4 7	1 10	5 6
1	3 8	1 10		5 6					5 6		1 10
2		3 8				2 9	2 9				3 8
3	1 10	2 9			4 7			4 7			2 9
4	2 9		4 7	3 8					3 8	4 7	
5	5 6		2 9			1 10	1 10			2 9	
6			3 8		1 10			1 10		3 8	
7				1 10		4 7	4 7		1 10		
8				2 9	5 6			5 6	2 9		
9	4 7				3 8	5 6	5 6	3 8			
10		4 7	5 6							5 6	4 7
$-\frac{a}{2}$	0	5	10	4	9	3	8	2	7	1	6

A chaque valeur, ajoutons $-\frac{a}{2}$ et nous avons le Tableau suivant (*fig.* 51) :

Valeurs de A et de B, cas de R carré, module 11.

Fig. 51.

a \ b	0	1	2	3	4	5	6	7	8	9	10
0		0 10	0 9	0 8	0 7	0 6	0 5	0 4	0 3	0 2	0 1
1	3 8	4 6		9 10					1 2		5 7
2		2 8				1 5	6 10				3 9
3	1 10	3 7			2 5			6 9			4 8
4	2 9		3 6	1 7					4 10	5 8	
5	5 6		1 8			2 4	7 9			3 10	
6			2 7		8 10			1 3		4 9	
7				3 5		7 10	1 4		6 8		
8				2 6	3 4			7 8	5 9		
9	4 7				1 6	8 9	2 3	5 10			
10		1 9	5 4							6 7	2 10

Il s'agit maintenant de prendre les racines cubiques de A et de B.

Pour cela nous allons employer (*fig.* 52) la Table des puissances des imaginaires du deuxième ordre, qui comprend 120 termes ($m^2 - 1$). Ce nombre $120 = 2^3.3.5$ sera donc *le module des indices.*

La Table a été construite en prenant pour équation réductrice $x^2+9=0$, dans laquelle le premier membre est une fonction irréductible du deuxième degré; nous avons donc $i^2=2$.

La base de la Table est l'imaginaire du deuxième ordre,

$$i^2+2i^0 \quad \text{ou} \quad 12,$$

suivant notre notation.

Pour la commodité de l'exposition j'ai mis 12 termes dans chaque ligne du Tableau; de cette façon les cubes, ou imaginaires à indices multiples de 3, seront tous contenus dans les colonnes de rang 3, 6, 9, 12; leurs racines cubiques seront ainsi plus faciles à calculer.

Un coup d'œil jeté sur la Table nous montre que tous les chiffres sont contenus dans la colonne de rang 12.

Table des imaginaires du deuxième degré, module 11.
Équation réductrice $i^2 = 2$.

Fig. 52.

Indices.	1	2	3	4	5	6	7	8	9	10	11	12
Imaginaires.	12	46	39	42	$\underline{10}$ 1	$\underline{10}$ 0	99	53	25	93	$\underline{10}$ 2	02
Cases.	72	$\underline{10}$ 4	48	75	9 $\underline{10}$	09	47	53	16	51	57	07
Indices.	13	14	15	16	17	18	19	20	21	22	23	24
Imaginaires.	24	81	67	84	92	90	77	$\underline{10}$ 6	4 $\underline{10}$	76	94	04
Cases.	38	95	8 $\underline{10}$	39	77	03	86	$\underline{10}$ 1	22	$\underline{10}$ 4	38	06
Indices.	25	26	27	28	29	30	31	32	33	34	35	36
Imaginaires.	48	52	13	58	74	70	33	91	89	31	78	08
Cases.	6 $\underline{10}$	79	57	63	36	01	52	94	48	95	6 $\underline{10}$	02
Indices.	37	38	39	40	41	42	43	44	45	46	47	48
Imaginaires.	85	$\underline{10}$ 4	26	$\underline{10}$ 5	38	30	66	72	57	62	35	05
Cases.	17	33	$\underline{10}$ 6	11	62	04	$\underline{10}$ 8	75	8 $\underline{10}$	79	17	08
Indices.	49	50	51	52	53	54	55	56	57	58	59	60
Imaginaires.	5 $\underline{10}$	98	41	9 $\underline{10}$	65	60	11	34	$\underline{10}$ 3	14	6 $\underline{10}$	0 $\underline{10}$
Cases.	26	61	92	24	18	05	9 $\underline{10}$	39	57	33	26	0 $\underline{10}$

Table des imaginaires du deuxième degré, module 11 (suite). Équation réductrice $i^2 = 2$.

Fig. 52.

Indices.	61	62	63	64	65	66	67	68	69	70	71	72
Imaginaires.	$\underline{10}$ 9	75	82	79	1 $\underline{10}$	10	22	68	96	28	19	09
Cases.	42	14	78	45	2 $\underline{10}$	09	77	63	$\underline{10}$ 6	61	67	07
Indices.	73	74	75	76	77	78	79	80	81	82	83	84
Imaginaires.	97	3 $\underline{10}$	54	37	29	20	44	15	71	45	27	07
Cases.	88	25	3 $\underline{10}$	89	47	03	36	11	92	14	88	06
Indices.	85	86	87	88	89	90	91	92	93	94	95	96
Imaginaires	73	69	$\underline{10}$ 8	63	47	40	88	2 $\underline{10}$	32	8 $\underline{10}$	43	03
Cases.	5 $\underline{10}$	49	67	53	86	01	62	24	78	25	5 $\underline{10}$	02
Indices.	97	98	99	100	101	102	103	104	105	106	107	108
Imaginaires.	36	17	95	16	83	80	55	49	64	59	86	06
Cases.	$\underline{10}$ 7	83	16	$\underline{10}$ 1	52	04	18	45	3 $\underline{10}$	49	$\underline{10}$ 7	08
Indices.	109	110	111	112	113	114	115	116	117	118	119	120
Imaginaires.	61	23	7 $\underline{10}$	21	56	50	$\underline{10}$ $\underline{10}$	87	18	$\underline{10}$ 7	51	01
Cases.	96	51	22	94	$\underline{10}$ 8	05	2 $\underline{10}$	89	67	83	96	0 $\underline{10}$

Prendre la racine cubique d'un terme quelconque de la Table, c'est diviser son indice par 3 et prendre les termes correspondant aux quotients.

Rappelons rapidement les principes de ces opérations.

Soient :

D le dividende,
d le diviseur,
M un module composé.

Si D ne contient pas tous les facteurs communs à *d* et à M, l'opération est impossible; si ce fait ne se produit pas, soit Δ le diviseur commun, 1 ou tout autre chiffre différent de 0, entre D, *d*, M, il y aura Δ solutions.

L'opération s'exécutera en supprimant partout le facteur Δ; soient D_1, d_1, M_1 les quotients; on exécutera la division de D_1 par d_1 module M_1 et au résultat unique, toujours possible, on ajoutera tous les multiples de $\frac{M}{\Delta}$, ce qui donnera les quotients. Prenant alors sur la Table les termes correspondant à ces indices, on aura les racines d'indice *d* du terme correspondant au dividende D.

Pour le cas actuel $d = 3$, tous les chiffres sont dans la colonne de rang 12; leurs indices sont donc divisibles par 3.

Prenons comme exemple 7 qui a pour indice 84; prenant le tiers de 84, nous avons 28; ajoutons-lui 40 et 80 et prenons les termes correspondants, nous avons le Tableau ci-dessous :

28	68	108	Indices.
58	68	06	Puissances.

Prenons maintenant (*fig.* 51) une case au hasard, soit 11 par exemple; nous y trouvons (4, 6).

Si l'un des chiffres représente A, l'autre représentera B.

Calculons les racines cubiques par le procédé ci-dessus.

24	8	48	88	Indices.
04	53	05	63	Puissances.

108	36	76	116	Indices.
06	08	37	87	Puissances.

En associant les trois racines cubiques de A et de B, nous aurions neuf combinaisons; mais, en Arithmétique comme en Algèbre, on ne doit prendre que les combinaisons dont le produit donne le chiffre $-\frac{b}{3}$.

Faisons la Table de multiplication, en prenant comme argument d'un côté les racines cubiques de A et de l'autre les racines cubiques de B, et calculons les produits en opérant sur les indices; nous avons le Tableau suivant ([1]) :

	$\frac{8}{53}$	$\frac{48}{05}$	$\frac{88}{63}$
$\frac{36}{08}$	$\frac{44}{72}$	$\frac{84}{07}$	$\frac{4}{42}$
$\frac{76}{37}$	$\frac{84}{07}$	$\frac{4}{42}$	$\frac{44}{72}$
$\frac{116}{87}$	$\frac{4}{42}$	$\frac{44}{72}$	$\frac{84}{07}$

Nous devons sur ce Tableau faire la somme des termes dont le produit $= 7$.

([1]) Dans ce Tableau et dans les analogues, quand dans une case il y a deux nombres séparés par un trait, le nombre supérieur est l'indice sur la Table des puissances du nombre inférieur, qui est une imaginaire du 2e degré.

Nous avons ainsi le Tableau suivant :

5 + 8	53 + 37	63 + 87	**Termes.**
2	8 $\underline{10}$	3 $\underline{10}$	**Sommes.**

Nous avons

$$- = - \frac{b}{3},$$

d'où

$$-b = 10 \qquad \text{et} \qquad b = 1.$$

Les trois termes ci-dessus, dont un réel et deux imaginaires du deuxième ordre, devront donc être inscrits dans la case 1011 (*fig.* 48).

Si, des racines, nous passons aux fonctions irréductibles qu'elles résolvent, nous trouvons que 2 résout l'équation $19 = 0$, et que les deux autres solutions imaginaires résolvent l'équation $125 = 0$.

Si nous multiplions 19 par 125 nous trouvons 1011 comme produit; si maintenant, nous regardons le plan arithmétique des solutions réelles, nous y trouvons le chiffre 2, case 11 (*fig.* 48).

Ainsi, il y a conformité absolue comme on devait s'y attendre.

Prenons toute autre case, il en sera de même; par suite, *dans le cas où* R *est un carré, il y a une solution réelle et deux solutions imaginaires du deuxième ordre.*

Ici, comme partout, nous trouvons, *mutatis mutandis,* une analogie complète avec la discussion de la formule de Cardan en Algèbre.

Dans les fonctions algébriques, si l'on fait toutes les combinaisons possibles de $\sqrt[3]{A}$ et de $\sqrt[3]{B}$, en appelant 1, α, β, les $\sqrt[3]{1}$, on trouve que ces combinaisons résolvent les trois équations

$$x^3 + (1, \alpha, \beta) bx + a = 0:$$

En Arithmétique, module 11, on a

$\sqrt[3]{1} =$

1	2	3	
01	$\underline{10}$ 5	15	Imaginaires.
120	40	80	Indices.

Si nous multiplions 07 dont l'indice est 84 par les racines cubiques de 01, nous obtenons :

07	42	72	Imaginaires.
84	4	44	Indices.

qui sont précisément les imaginaires que nous trouvons dans la Table de multiplication comme valeurs de $\sqrt[3]{\overline{AB}}$.

Faisons la somme des imaginaires dont le produit égale (42, 72)

42	08 63	37 05	87 53	72	08 53	37 63	87 05	
	60	31	2 $\underline{10}$		50	9 $\underline{10}$	81	Sommes.

Nous trouvons pour $-\frac{b}{3} = 42$ les solutions

(60, 31, 2 $\underline{10}$),

et pour $-\frac{b}{3} = 72$ les solutions

(50, 9 $\underline{10}$, 81).

Si nous passons de $-\frac{b}{3}$ à b nous avons

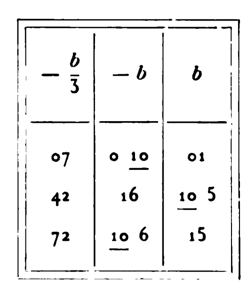
(1, $\underline{10}$ 5, 15),

c'est-à-dire

$$1 \times 1, \qquad 1 \times \alpha, \qquad 1 \times \beta;$$

nos équations sont, par suite,

$$x^3 + (01, \underline{10}\,5, 15)x + a = 0.$$



$-\frac{b}{3}$	$-b$	b
07	0 $\underline{10}$	01
42	16	$\underline{10}$ 5
72	$\underline{10}$ 6	15

L'analogie est donc absolue.

Faisons maintenant le dénombrement des cas où R est un carré.

Jetons un coup d'œil sur la figure 51; nous y trouvons toutes les associations possibles d'un chiffre quelconque avec un chiffre quelconque, en nombre,

$$\frac{10.11}{1.2} = 55;$$

dans notre Table des puissances des imaginaires du deuxième ordre, il y a $m^2 - m = 110$ imaginaires du deuxième ordre, chaque collection de racines en contient 2; nous trouvons donc le nombre 55.

Considérons maintenant le cas où $R = 0$, soit, par exemple, case 23; nous avons

$$a = 3, \qquad -a = 8, \qquad -\frac{a}{2} = 4 \ (\textit{fig. } 49).$$

Si nous prenons les racines cubiques de 4, nous trouvons :

24	8	48	88	Indices.
04	53	05	63	Puissances.

A et B sont, dans ce cas, identiques.

Formons la Table de multiplication :

	$\frac{8}{53}$	$\frac{48}{05}$	$\frac{88}{63}$
$\frac{8}{53}$	$\frac{16}{84}$	$\frac{56}{34}$	$\frac{96}{03}$
$\frac{48}{05}$	$\frac{56}{34}$	$\frac{96}{03}$	$\frac{16}{84}$
$\frac{88}{63}$	$\frac{96}{03}$	$\frac{16}{84}$	$\frac{56}{34}$

Faisant la somme des termes dont le produit $= 3$, nous avons le Tableau suivant :

53 + 63	05 + 05	63 + 53	Termes.
06	0 $\underline{10}$	06	Sommes.

Nous trouvons donc, dans ce cas, *trois racines réelles dont deux égales*, et, comme la somme $-c$ des racines est égale à zéro, *le complément de l'une d'elles est égal au double de chacune des autres*.

Prenons notre plan arithmétique des solutions réelles, nous trouvons, case 1023, les trois chiffres (6, 6, 10).

Quant au dénombrement des cas, il est de

$$(m - 1) = 10.$$

Prenons maintenant le cas de R non carré. Les racines carrées d'un chiffre non carré sont des imaginaires du deuxième ordre; si nous leur ajoutons $-\frac{a}{2}$, nous avons le Tableau de la figure 53 :

Valeurs de A et de B, cas de R non carré. Module 11.

Fig. 53.

$-\frac{a}{2}$	0	5	10	4	9	3	8	2	7	1	6
a	0	1	2	3	4	5	6	7	8	9	10
b											
0											
1			7 $\underline{10}$ 4 $\underline{10}$		$\underline{10}$ 9 19	33 83	38 88	$\underline{10}$ 2 12		71 41	
2	6 0 5 0		3 $\underline{10}$ 8 $\underline{10}$		79 49			72 42		31 81	
3			10 $\underline{10}$ 1 $\underline{10}$	54 64		43 73	48 78		57 67	$\underline{10}$ 1 11	
4		35 85			29 99	13 $\underline{10}$ 3	18 $\underline{10}$ 8	22 92			36 86
5		55 65		24 94	39 89			32 82	27 97		56 66
6	9 0 2 0			14 $\underline{10}$ 4		53 63	58 68		17 $\underline{10}$ 7		
7	3 0 8 0	45 75	2 $\underline{10}$ 9 $\underline{10}$							21 91	46 76
8	7 0 4 0	15 $\underline{10}$ 5				23 93	28 98				16 $\underline{10}$ 6
9		25 95	5 $\underline{10}$ 6 $\underline{10}$	44 74					47 77	51 61	26 96
10	$\underline{10}$ 0 1 0			34 84	59 69			52 62	37 87		

Mais ici nous nous trouvons en face d'un nouvel ordre de considérations :

Si nous regardons la Table des puissances des imaginaires du deuxième ordre, nous trouvons dans les colonnes de rang (3, 6, 9) trente imaginaires dont l'indice est divisible par 3 ; ces imaginaires ont pour racines cubiques trois imaginaires de la même Table. Elles correspondent aux cases que nous avons entourées d'un carré. En pratiquant sur ces imaginaires les calculs dont nous avons donné un spécimen ci-dessus, les résultats du calcul donnent trois racines réelles ; je m'abstiens de ce calcul que le lecteur peut exécuter avec facilité puisqu'il a les éléments nécessaires pour le faire ; il pourra de plus constater la concordance des résultats avec le plan des solutions réelles.

Dans le cas des imaginaires de la forme $((m))$ qui sont contenues dans la colonne du Tableau dans laquelle $a = 0$, la troisième solution réelle est 0, les deux autres étant des chiffres différents de 0 et inégaux.

Si maintenant nous prenons les quarante cases restantes, les quatre-vingts imaginaires contenues dans les colonnes de rangs 1, 2, 4, 5, 7, 8, 10, 11 de la Table des puissances, leurs indices ne sont pas divisibles par 3, leurs racines cubiques ne sont donc pas des termes de la Table des imaginaires du deuxième ordre, mais des imaginaires du troisième.

Les cases que ce cas concerne sont des cases blanches correspondant à des fonctions irréductibles du troisième degré. Le nombre de ces fonctions est de $\frac{m^3 - m}{3}$ pour l'équation complète ; comme ces cases blanches sont également réparties dans tous les plans, il y en a par suite

$$\frac{m^2 - 1}{3} = \frac{120}{3} = 40$$

pour le plan $10ba$.

Seulement il est à remarquer ici que la Table des imaginaires du troisième ordre ne contient pas d'imaginaires du deuxième.

Résumons ce qui précède : *si* R = *non carré, on a tantôt trois racines réelles inégales, tantôt trois racines imaginaires du troisième ordre inégales.*

Il n'est peut-être pas inutile de rappeler ici que *les imaginaires*

algébriques étant des longueurs dirigées, situées en dehors de la direction de référence, il ne peut y avoir que des imaginaires du deuxième ordre, tandis qu'il existe des imaginaires de tous les ordres dans les fonctions arithmétiques, celles-ci résolvant les fonctions irréductibles de même degré.

Je n'ai pas besoin de faire remarquer l'importance de cette observation, que la formule de Cardan appliquée aux fonctions arithmétiques fait ressortir dans tout son éclat.

Formule de Cardan; module $3n+1$.

80. Étudions maintenant les modules de la forme $3n+1$, c'est-à-dire tels que $(m-1)$ est divisible par 3. Je choisirai le module 13 pour montrer l'application de la formule de Cardan.

Nous donnons d'abord (*fig.* 54) le plan arithmétique $10ba$ correspondant à l'équation

$$x^3+bx+a\equiv 0.$$



Équation $x^3 + bx + a = 0$. Solutions réelles. Module 13.

Fig. 54.

a \ b	0	1	2	3	4	5	6	7	8	9	10	11	12
0	00 0	4, $\underline{10}$ $\underline{12}$				2, 5 6			7, 8 $\underline{11}$				1, 3 9
1	0 5, 8	7	$\underline{12}$	2, 2 9	$\underline{10}$					3	4, 4 $\underline{11}$	1	6
2	0	2		$\underline{12}$		8	3, 4 6	7, 9 $\underline{10}$	5		1		$\underline{11}$
3	0 6, 7	$\underline{11}$	4	5, 5 3	$\underline{12}$					1	8, 8 $\underline{10}$	9	2
4	0 3, $\underline{10}$		9, 9 8	$\underline{11}$		$\underline{12}$	7	6	1		2	4, 4 5	
5	0	6		$\underline{10}$		$\underline{11}$	5, 9 $\underline{12}$	1, 4 8	2		3		7
6	0	5		4		7	1, 2 $\underline{10}$	3, $\underline{11}$ $\underline{12}$	6		9		8
7	0	9	6		2, 3 8	1			$\underline{12}$	5, $\underline{10}$ $\underline{11}$		7	4
8	0	3	2		1, 5 7	9			4	6, 8 $\underline{12}$		$\underline{11}$	$\underline{10}$
9	0 2, $\underline{11}$	8	$\underline{10}$	6, 6 1	4					9	7, 7 $\underline{12}$	3	5
10	0 4, 9		1, 1 $\underline{11}$	7		$\underline{10}$	8	5	3		6	$\underline{12}$ $\underline{12}$ 2	
11	0	1	5		6, 9 $\underline{11}$	3			$\underline{10}$	2, 4 7		8	$\underline{12}$
12	0 1, $\underline{12}$		3, 3 7	8		4	$\underline{11}$	2	9		5	$\underline{10}$ $\underline{10}$ 7	

Voici maintenant (*fig.* 55) le Tableau contenant les valeurs de R :

Valeur de R, formule de Cardan. Module 13.

Fig. 55.

		0	1	2	3	4	5	6	7	8	9	$\underline{10}$	$\underline{11}$	$\underline{12}$	a
		0	$\underline{10}$	1	$\underline{12}$	4	3	9	9	3	4	$\underline{12}$	1	$\underline{10}$	$\frac{a^2}{4}$
0	0	0	$\underline{10}$	1	$\underline{12}$	4	3	9	9	3	4	$\underline{12}$	1	$\underline{10}$	
1	1	1	$\underline{11}$	2	0	5	4	$\underline{10}$	$\underline{10}$	4	5	0	2	$\underline{11}$	
2	8	8	5	9	7	$\underline{12}$	$\underline{11}$	4	4	$\underline{11}$	$\underline{12}$	7	9	5	
3	1	1	$\underline{11}$	2	0	5	4	$\underline{10}$	$\underline{10}$	4	5	0	2	$\underline{11}$	
4	$\underline{12}$	$\underline{12}$	9	0	$\underline{11}$	3	2	8	8	2	3	$\underline{11}$	0	9	
5	8	8	5	9	7	$\underline{12}$	$\underline{11}$	4	4	$\underline{11}$	$\underline{12}$	7	9	5	
6	8	8	5	9	7	$\underline{12}$	$\underline{11}$	4	4	$\underline{11}$	$\underline{12}$	7	9	5	
7	5	5	2	6	4	9	8	1	1	8	9	4	6	2	
8	5	5	2	6	4	9	8	1	1	8	9	4	6	2	
9	1	1	$\underline{11}$	2	0	5	4	$\underline{10}$	$\underline{10}$	4	5	0	2	$\underline{11}$	
$\underline{10}$	$\underline{12}$	$\underline{12}$	9	0	$\underline{11}$	3	2	8	8	2	3	$\underline{11}$	0	9	
$\underline{11}$	5	5	2	6	4	9	8	1	1	8	9	4	6	2	
$\underline{12}$	$\underline{12}$	$\underline{12}$	9	0	$\underline{11}$	3	2	8	8	2	3	$\underline{11}$	0	9	
b	$\frac{b^3}{27}$														

Prenons d'abord le cas de R carré.

La racine carrée de R se compose de deux chiffres; en leur ajoutant $-\frac{a}{2}$, on trouve le Tableau (*fig.* 56) des valeurs de A et de B.

Valeurs de A et de B. Cas de R carré. Module 13.

Fig. 56.

a \ b	0	1	2	3	4	5	6	7	8	9	10	11	12
0		0 12	0 11	0 10	0 9	0 8	0 7	0 6	0 5	0 4	0 3	0 2	0 1
1	1 12					2 6	3 4	9 10	7 11				
2			2 9		3 6		12 8	1 5		7 10		4 11	
3	1 12					2 6	3 4	9 10	7 11				
4	5 8	3 9			2 7					6 11			4 10
5			2 9		3 6		12 8	1 5		6 11		4 11	
6			2 9		3 6		12 8	1 5		6 11		4 11	
7				3 7	1 8		9 11	2 4		5 12	6 10		
8				3 7	1 8		9 11	2 4		5 12	6 10		
9	1 12					2 6	3 4	9 10	7 11				
10	5 8	3 9			2 7					6 11			4 10
11				3 7	1 8		9 11	2 4		5 12	6 10		
12	5 8	3 9			2 7					6 11			4 10

On ne peut associer ensemble que des chiffres dont le produit $AB = -\frac{b}{3}$, si l'on veut que les coefficients soient réels; c'est précisément ce que va nous montrer la formule de Cardan.

Comme $(m-1)$ est divisible par 3, il se passe ici un fait inverse à celui qui s'est produit pour le module 11; pour ce dernier, tout chiffre a une racine cubique réelle, tandis que, module 13, les chiffres se divisent en deux catégories; les cubes, qui ont trois racines cubiques réelles, et les non cubes, qui n'en ont aucune.

Nous étudierons séparément chaque catégorie.

Première catégorie. — Le chiffre sous le radical cubique est un cube.

Voici le Tableau des puissances de la racine primitive 2 :

1	2	3	4	5	6	7	8	9	10	11	0	Indices.
2	4	8	3	6	12	11	9	5	10	7	1	Puissances.

Puis les cubes et leurs racines cubiques :

1	5	8	12	Cubes.
1, 3, 9	7, 8, 11	2, 5, 6	4, 10, 12	Leurs racines cubiques.

Prenons au hasard une case à chiffres cubes, soit 74; nous y trouvons (1, 8) (*fig.* 56).

Formons la Table de multiplication de leurs racines cubiques :

	1	3	9
2	2	6	5
5	5	2	6
6	6	5	2

Les chiffres qui s'associeront pour former ensemble une solution seront ceux dont le produit donne un même chiffre pour $-\frac{b}{3}$.

Faisant leur somme, nous avons le Tableau :

$1+2$	$5+3$	$6+9$	$2+3$	$5+9$	$6+1$	$2+9$	$5+1$	$6+3$
3	8	2	5	1	7	11	6	9
$-\frac{b}{3}=2$		$b=7$	$-\frac{b}{3}=6$		$b=8$	$-\frac{b}{3}=5$		$b=11$

dans lequel j'ai indiqué la valeur de b.

Ainsi les solutions (2, 3, 8) seront situées case 1074; (1, 5, 7) case 1084; (6, 9, 11) case 10 11 5, comme on peut s'en assurer sur le plan des solutions réelles (*fig.* 54).

Le lecteur remarquera que, dans chaque colonne de la figure 56, chaque association de chiffres est répétée trois fois, correspondant ainsi à trois valeurs de b associées à la même valeur de a.

Passons au cas où le chiffre sous le radical cubique est un non cube.

Pour que $-\frac{b}{3}$ soit réel, il faut que AB soit un cube, ce qui exige que l'un des chiffres ait un indice de la forme $3n+1$ et l'autre un indice de la forme $3n+2$.

1	4	7	10		2	5	8	11	Indices.
2	3	11	10		4	6	9	7	Puissances.

Voilà le Tableau des chiffres de chaque catégorie; le nombre des associations possibles sera de $4 \times 4 = 16$, qui répété trois fois donnera 48 associations.

Ces 48 associations correspondent, ainsi que le lecteur peut s'en assurer, aux cases blanches du plan arithmétique donnant toutes les solutions réelles. Autrement dit, les polynomes correspondant à ces cases sont des fonctions irréductibles du troisième ordre, n'ayant pour solutions que des imaginaires de cet ordre.

Pour obtenir ces racines, il n'y a qu'à opérer sur la Table des puissances des imaginaires du troisième ordre, en exécutant les opérations d'une façon analogue à celles dont nous avons donné des spécimens ci-dessus, et procédant au moyen des indices.

Les divers chiffres, ainsi que je l'ai montré pour le module 7, ont tous des indices multiples de $\frac{m^3-1}{m-1}$; ceux qui sont des cubes ont des indices multiples de 3; le module des indices étant divisible par 3, ces indices, divisés par 3, donneront trois indices réels, et l'on n'aura qu'à prendre les termes de la Table correspondant aux quotients, et sur ces termes faire la Table de multiplication; la somme des termes du cadre correspondant au même produit, qui est égal à $-\frac{b}{3}$, donnera les imaginaires à loger dans chaque case.

Si, maintenant, nous considérons le cas où $b = 0$, l'expression sous le radical devient

$$-\frac{a}{2} \pm \sqrt[2]{\frac{a^2}{4}};$$

c'est-à-dire

$$-\frac{a}{2} \pm \frac{a}{2};$$

l'une des valeurs est $-a$ et l'autre o.

L'un des radicaux cubiques contiendra $-a$, l'autre o; leur somme sera donc $\sqrt[3]{-a}$.

Si $-a$ est un cube, on aura trois solutions du premier ordre; si $-a$ est un non cube, il en résultera une case blanche, n'ayant pour solution que des imaginaires du troisième ordre; ce dont on peut s'assurer sur la figure 54.

Ces valeurs sont au nombre de 8. En ajoutant $48 + 8 = 56$, on a le nombre des fonctions irréductibles du troisième degré qui est de $\frac{m^3 - m}{3}$ pour l'équation complète, et ici de $\frac{m^2 - 1}{3} = \frac{168}{3} = 56$.

Ainsi, *lorsque* $(m - 1)$ *est divisible par* 3, *si* R *est un carré, on a tantôt trois racines réelles, tantôt trois racines imaginaires.*

Passons au cas où $R = 0$.

Si $\frac{a^2}{4} + \frac{b^3}{27} = 0$, on a

$$\frac{a^2}{4} = -\frac{b^3}{27};$$

b étant réel, $\frac{b^3}{27}$ et $-\frac{b^3}{27}$ sont des cubes; $\frac{a^2}{4}$ est donc un cube et $\pm\frac{a}{2}$ également; ses racines cubiques sont des chiffres, et A et B seront identiques.

Prenons au hasard une des cases, soit 1042;

$$a = 2, \qquad -\frac{a}{2} = \frac{11}{2} = 12;$$

les racines cubiques de 12 sont 4, $\underline{10}$, $\underline{12}$; faisons la Table de multiplication :

	4	10	12
4	3	1	9
10	1	9	3
12	9	3	1

Formons aussi la somme des chiffres du cadre correspondant à un même produit :

$4+4$	$\underline{10}+\underline{12}$	$10+12$	$4+10$	$10+4$	$12+12$	$4+12$	$10+10$	$4+12$
8	9	9	1	1	11	3	7	3
$-\frac{b}{3}=3$		$b=4$	$-\frac{b}{3}=1$		$b=10$	$-\frac{b}{3}=9$		$b=12$

Ainsi, *pour* $R=0$, *il y a trois racines réelles dont deux égales,* ce dont on peut s'assurer sur le plan arithmétique donnant les solutions réelles. La somme des solutions étant égale à 0 dans le plan $10ba$, l'une d'elles est égale au complément du double de chacune des autres. Le nombre des cas est de $13=m$.

Cas où R *est non carré.* — Sa racine carrée est une imaginaire du deuxième ordre.

Nous donnons (*fig.* 57) la Table de puissances de ces imaginaires pour le module 13 en prenant pour équation réductrice $i^2=2$ ou $x^2+11=0$, et pour base $i+2$ ou 12.

Table des imaginaires du deuxième degré, module 13.
Équation réductrice $i^2 = 2$.

Fig. 57.

Indices.	1	2	3	4	5	6	7	8	9	10	11	12
Imaginaires.	12	46	17	93	8 $\underline{11}$	1 $\underline{12}$	10	22	68	72	35	11 3
Cases.	93	17	$\underline{12}$ 9	76	45	20	0 $\underline{12}$	90	$\underline{10}$ 2	97	33	75
Indices.	13	14	15	16	17	18	19	20	21	22	23	24
Imaginaires.	$\underline{12}$ 2	02	24	8 $\underline{12}$	21	56	39	2 $\underline{11}$	20	44	$\underline{12}$ 3	14
Cases.	93	94	5 $\underline{12}$	22	$\underline{11}$ $\underline{10}$	1 $\underline{11}$	87	40	09	50	78	52
Indices.	25	26	27	28	29	30	31	32	33	34	35	36
Imaginaires.	6 $\underline{10}$	96	$\underline{11}$ 4	04	48	3 $\underline{11}$	42	$\underline{10}$ $\underline{12}$	65	49	40	88
Cases.	6 $\underline{12}$	17	5 $\underline{12}$	53	$\underline{10}$ 9	48	91	25	32	80	0 $\underline{10}$	$\underline{10}$ 0
Indices.	37	38	39	40	41	42	43	44	45	46	47	48
Imaginaires.	$\underline{11}$ 6	28	$\underline{12}$ 7	5 $\underline{12}$	98	08	83	69	84	7 $\underline{11}$	$\underline{12}$ $\underline{10}$	85
Cases.	16	$\underline{10}$ 8	$\underline{12}$ 9	22	$\underline{10}$ 9	$\underline{10}$ $\underline{12}$	71	86	54	47	68	30
Indices.	49	50	51	52	53	54	55	56	57	58	59	60
Imaginaires.	80	33	9 $\underline{12}$	43	$\underline{11}$ 1	$\underline{10}$ $\underline{11}$	53	03	36	$\underline{12}$ 5	38	19
Cases.	01	70	2 $\underline{11}$	76	$\underline{11}$ $\underline{10}$	48	7 $\underline{10}$	79	11	3 $\underline{11}$	$\underline{10}$ 3	82
Indices.	61	62	63	64	65	66	67	68	69	70	71	72
Imaginaires.	$\underline{11}$ 7	3 $\underline{10}$	30	66	5 $\underline{11}$	86	92	79	$\underline{10}$ 6	06	6 $\underline{12}$	$\underline{11}$ $\underline{10}$
Cases.	$\underline{12}$ 6	60	04	10	45	1 $\underline{11}$	91	86	11	1 $\underline{10}$	24	65
Indices.	73	74	75	76	77	78	79	80	81	82	83	84
Imaginaires.	63	25	91	67	60	$\underline{12}$ $\underline{12}$	$\underline{10}$ 9	3 $\underline{12}$	54	15	7 $\underline{12}$	0 $\underline{12}$
Cases.	7 $\underline{12}$	38	$\underline{11}$ $\underline{11}$	$\underline{12}$ 0	03	20	87	25	54	3 $\underline{11}$	24	21

Table des imaginaires du deuxième degré, module 13 (suite).
Équation réductrice $i^2 - 2$.

Fig. 57.

Indices.	85	86	87	88	89	90	91	92	93	94	95	96
Imaginaires.	$\underline{12}\ \underline{11}$	97	$\underline{12}$ 6	4 $\underline{10}$	52	$\underline{12}$ 1	12 0	$\underline{11}\ \underline{11}$	75	6 $\underline{11}$	$\underline{10}$ 8	2 $\underline{10}$
Cases.	43	$\underline{12}$ 7	19	66	95	$\underline{11}$ 0	0 $\underline{12}$	40	32	47	$\underline{10}$ 3	95
Indices.	97	98	99	100	101	102	103	104	105	106	107	108
Imaginaires.	1 $\underline{11}$	0 $\underline{11}$	$\underline{11}$ 9	51	$\underline{11}\ \underline{12}$	87	$\underline{10}$ 4	$\underline{11}$ 2	$\underline{11}$ 0	99	1 $\underline{10}$	$\underline{12}$ 9
Cases.	43	44	81	$\underline{11}$ 2	2 $\underline{10}$	$\underline{12}\ \underline{11}$	57	90	09	80	68	82
Indices.	109	110	111	112	113	114	115	116	117	118	119	120
Imaginaires.	73	47	29	09	95	$\underline{10}$ 2	9 $\underline{11}$	31	78	94	90	55
Cases.	7 $\underline{12}$	$\underline{12}$ 7	8 $\underline{12}$	83	39	98	41	$\underline{11}$ 5	$\underline{10}$ 2	50	0 $\underline{10}$	30
Indices.	121	122	123	124	125	126	127	128	129	130	131	132
Imaginaires.	27	$\underline{11}$ 5	16	81	45	05	5 $\underline{10}$	74	59	62	13	58
Cases.	$\underline{12}$ 6	38	19	$\underline{11}$ 2	39	3 $\underline{12}$	6 $\underline{10}$	56	84	97	78	$\underline{10}$ 0
Indices.	133	134	135	136	137	138	139	140	141	142	143	144
Imaginaires.	50	$\underline{10}\ \underline{10}$	41	9 $\underline{10}$	2 $\underline{12}$	32	8 $\underline{10}$	0 $\underline{10}$	$\underline{10}$ 7	18	$\underline{10}$ 5	$\underline{12}$ 4
Cases.	01	60	$\underline{11}\ \underline{11}$	66	2 $\underline{10}$	98	6 $\underline{10}$	69	$\underline{12}$ 1	$\underline{10}\ \underline{11}$	33	52
Indices.	145	146	147	148	149	150	151	152	153	154	155	156
Imaginaires.	26	$\underline{10}$ 3	$\underline{10}$ 0	77	82	57	4 $\underline{11}$	64	37	07	71	23
Cases.	16	70	04	$\underline{12}$ 0	95	$\underline{12}\ \underline{11}$	41	56	$\underline{12}$ 1	$\underline{12}\ \underline{10}$	$\underline{11}$ 4	75
Indices.	157	158	159	160	161	162	163	164	165	166	167	168
Imaginaires.	7 $\underline{10}$	$\underline{11}$ 8	4 12	76	70	11	34	10 1	89	$\underline{12}$ 8	61	01
Cases.	6 $\underline{12}$	$\underline{10}$ 8	2 $\underline{11}$	10	03	$\underline{11}$ 0	57	$\underline{11}$ 5	84	$\underline{10}\ \underline{11}$	$\underline{11}$ 4	$\underline{11}$ 1

Ajoutons $-\frac{a}{2}$ aux valeurs de $\sqrt[2]{R}$ et nous avons le Tableau de la figure 58 :

Valeurs de A et de B quand R est non carré, module 13.

Fig. 58.

		0	6	12	5	11	4	10	3	9	2	8	1	7	—
		0	1	2	3	4	5	6	7	8	9	10	11	12	a
0	0														
4	1		56 86	1 12 12 12		3 11 10 11					32 10 2		11 12 1	57 87	
8	2	2 . 11 .	36 10 6		65 75		54 84			59 89		68 78		37 10 7	
12	3		56 86	1 12 12 12		3 11 10 11					32 10 2		11 12 1	57 87	
3	4				55 85		14 12 4	2 10 11 10	23 11 3	19 12 9		58 88			
7	5	2 . 11 .	36 10 6		65 75		54 84			59 89		68 78		37 10 7	
11	6	2 . 11 .	36 10 6		65 75		54 84			59 89		68 78		37 10 7	
2	7	3 . 10 .	16 12 6	4 12 9 12			24 11 4			29 11 9			41 91	17 12 7	
6	8	3 . 10 .	16 12 6	4 12 9 12			24 11 4			29 11 9			41 91	17 12 7	
10	9		56 86	1 12 12 12		3 11 10 11					32 10 2		11 12 1	57 87	
1	10				55 85		14 12 4	2 10 11 10	23 11 3	19 12 9		58 88			
5	11	3 . 10 .	16 12 6	4 12 9 12			24 11 4			29 11 9			41 91	17 12 7	
9	12				55 85		14 12 4	2 10 11 10	23 11 3	19 11 9		58 88			

$-\frac{b}{3}$ $\quad b$

Jetons un coup d'œil sur ce Tableau; nous voyons qu'il y a 78 cases remplies. Dans chaque colonne les mêmes associations de chiffres sont répétées trois fois; il y a donc en tout 26 associations différentes, chaque case contient 2 imaginaires associées; total 52.

Or c'est précisément là le nombre des imaginaires dont l'indice est un multiple de 3 sur la Table des puissances.

L'indice étant un multiple de 3, la racine cubique est un terme de la même Table, c'est-à-dire une imaginaire du deuxième ordre.

Prenons au hasard une case quelconque et faisons les calculs; soit, par exemple, la case 11; nous trouvons (56, 86) (*fig.* 58).

56 a pour indice 18.

Indices.	18	6	62	118	66	22	78	134
Imaginaires.	56	$1\ \underline{12}$	$3\ \underline{10}$	94	86	44	$\underline{12}\ \underline{12}$	$\underline{10}\ \underline{10}$
		Racines cubiques.				Racines cubiques.		

Pour avoir les racines cubiques, prenons le tiers de chaque indice; ajoutons-lui 56 et 112 multiples du tiers du module des indices 168, et nous avons le Tableau ci-dessus.

Maintenant faisons la Table de multiplication, en nous aidant des indices dans le calcul.

Faisons de plus la somme des radicaux résolvant une même équation, et nous avons les Tableaux suivants :

	$\frac{6}{1\ \underline{12}}$	$\frac{62}{3\ \underline{10}}$	$\frac{118}{94}$
$\frac{22}{44}$	$\frac{28}{04}$	$\frac{84}{0\ \underline{12}}$	$\frac{140}{0\ \underline{10}}$
$\frac{78}{\underline{12}\ \underline{12}}$	$\frac{84}{0\ \underline{12}}$	$\frac{140}{0\ \underline{10}}$	$\frac{28}{04}$
$\frac{134}{\underline{10}\ \underline{10}}$	$\frac{140}{0\ \underline{10}}$	$\frac{28}{04}$	$\frac{84}{0\ \underline{12}}$

$1\ \underline{12} + 44$	$\underline{12}\ \underline{12} + 94$	$\underline{10}\ \underline{10} + 3\ \underline{10}$
53	83	07
$3\ \underline{10} + 44$	$\underline{12}\ \underline{12} + 1\ \underline{12}$	$\underline{10}\ \underline{10} + 94$
71	$0\ \underline{11}$	61
$94 + 44$	$\underline{12}\ \underline{12} + 3\ \underline{10}$	$\underline{10}\ \underline{10} + 1\ \underline{12}$
08	29	$\underline{11}\ 9$

$-\frac{b}{3}$	4	10	12
b	1	9	3
Solutions réelles.	7	8	11

Si l'on se rapporte à la figure 54, nous voyons que la case 1091 contient 8, la case 1031 contient 11, et la case 1011 contient 7, ainsi qu'il résulte du Tableau ci-dessus.

Quelle que soit la case que l'on prenne il en sera toujours de même, c'est-à-dire que, *pour le cas de* R $=$ *non carré, il y a une solution réelle et deux solutions imaginaires du deuxième ordre.*

Comme complément à ce qui précède, je vais appliquer la formule de Cardan au cas où $a = 0$.

Dans ce cas la formule devient

$$\left|\sqrt[3]{+\sqrt[2]{\frac{b^3}{27}}}+\sqrt[3]{-\sqrt[2]{\frac{b^3}{27}}}\right| \left|\sqrt[3]{+\sqrt[2]{b^3}}+\sqrt[3]{-\sqrt[2]{b^3}}\right.,$$

$\frac{b^3}{27}$ équivalant congrument à b^3.

Si b est un carré, b^3 sera un carré; soit $b = 3$, on a

$$b^3 = 1,$$
$$\sqrt[2]{b^3} = (1, \underline{12}),$$
$$-\sqrt[2]{b^3} = (1, \underline{12}),$$
$$\sqrt[3]{1} = (1, 3, 9),$$
$$\sqrt[3]{12} = (4, \underline{10}, \underline{12}).$$

Faisons la Table de multiplication :

	1	3	9
4	4	12	10
10	10	4	12
12	12	10	4

1 + 4	10 + 3	12 + 9	4 + 3	10 + 9	12 + 1	4 + 9	10 + 1	12 + 3
5	0	8	7	6	0	0	11	2
$-\frac{b}{3} = 4$		$b = 1$	$-\frac{b}{3} = 12$		$b = 3$	$-\frac{b}{3} = 10$		$b = 9$

Si l'on se rapporte à la figure 54, on trouve bien les chiffres (0, 5, 8) à la case 1010, les chiffres (0, 6, 7) à la case 1030, les chiffres (0, 2, 11) à la case 1090.

Dans le cas où b n'est pas un carré, $\frac{b^3}{27}$ n'en est pas un, sa racine carrée est une imaginaire du deuxième ordre.

Prenons comme exemple $b = 2$, d'où $b^3 = 8$; si, sur la Table des imaginaires du deuxième ordre, nous prenons les racines carrées, et si nous extrayons ensuite les racines cubiques, nous avons le Tableau suivant :

Indices.	21	7	63	119	105	35	91	147
Imaginaires	2	10	30	90	$\underline{11}\,0$	40	$\underline{12}\,0$	$\underline{10}\,0$
		Racines cubiques.				Racines cubiques.		

Si maintenant nous faisons la Table de multiplication :

	$\frac{7}{10}$	$\frac{63}{30}$	$\frac{119}{90}$
$\frac{35}{40}$	$\frac{42}{8}$	$\frac{98}{11}$	$\frac{154}{7}$
$\frac{91}{\underline{12}\,0}$	$\frac{98}{11}$	$\frac{154}{7}$	$\frac{42}{8}$
$\frac{147}{\underline{10}\,0}$	$\frac{154}{7}$	$\frac{42}{8}$	$\frac{98}{11}$

et si nous formons la somme des imaginaires dont le produit est égal à une même quantité réelle, en écrivant que ce produit est égal à $-\frac{b}{3}$, nous avons les Tableaux suivants :

$10+40$	$\underline{12}\,0+35$	$\underline{12}\,0+90$
50	0	80
$-\frac{b}{3}=4$	$b=1$	

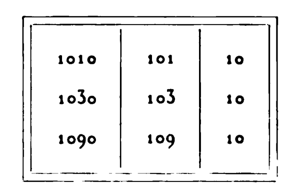
$40+30$	$\underline{10}\,0+90$	$\underline{12}\,0+10$
70	60	0
$-\frac{b}{3}=12$	$b=3$	

$40+90$	$\underline{10}\,0+10$	$\underline{12}\,0+80$
0	$\underline{11}\,0$	20
$-\frac{b}{3}=10$	$b=9$	

Les cases :

1010	doivent contenir	50	80	00
1030		70	60	00
1090		11 0	20	00

Comme vérification, on voit que la somme des imaginaires est nulle, et que le produit de ces imaginaires donne successivement 1, 3, 9; autrement dit, chaque case doit contenir les facteurs irréductibles donnés par le Tableau ci-dessous :



1010	101	10
1030	103	10
1090	109	10

Résumons maintenant dans un Tableau les résultats qui précèdent :

Fonctions arithmétiques.

Si $(m-1)$ n'est pas un multiple de 3 :

R = o	3 racines réelles dont 2 égales.
R = carré........	1 racine réelle et 2 racines imaginaires du deuxième ordre.
R = non carré...	Tantôt 3 racines réelles inégales, tantôt 3 racines imaginaires du troisième ordre inégales.

Si $(m-1)$ est un multiple de 3 :

R = o	3 racines réelles dont 2 égales.
R = non carré...	1 racine réelle et 2 racines imaginaires du deuxième ordre.
R = carré........	Tantôt 3 racines réelles inégales, tantôt 3 racines imaginaires du troisième ordre inégales.

Fonctions algébriques.

R = o	3 racines réelles dont 2 égales.
R positif.........	1 racine réelle, 2 racines imaginaires.
R négatif........	3 racines réelles et inégales.

Tables d'imaginaires du troisième ordre.

81. Supposons qu'une Table complète de puissances d'imaginaires i, i^2, ..., i^{m^3-1} ait été construite, en se servant de l'équation réductrice connue

$$x^3+cx^2+bx+a=0,$$

et qu'on se propose de savoir quelle est l'équation

$$x^3+c_kx^2+b_kx+a_k,$$

dont est racine un terme i^k de la Table.

Nous pouvons y arriver par le calcul des fonctions symétriques comme nous l'avons indiqué en général. Mais ce calcul est souvent

assez pénible; et, pour ce cas spécial du troisième degré, il est possible de résoudre la question d'une autre manière.

L'équation réductrice a pour racines i, i^m, i^{m^2}; l'équation cherchée, i^k, i^{km}, i^{km^2}. Donc

$$-a = i^{1+m+m^2}, \qquad -a_k = i^{k(1+m+m^2)} = (-a)^k.$$

De là, cette première relation

$$(1) \qquad a_k = -(-a)^k = (-1)^{k+1} a,$$

qui donne immédiatement le dernier terme.

Nous avons en outre

$$-c_k = i^k + i^{km} + i^{km^2}.$$

Or

$$\begin{aligned} -i^3 &= ci^2 + bi + a,\\ -i^{3m} &= ci^{2m} + bi^m + a,\\ -i^{3m^2} &= ci^{2m^2} + bi^{m^2} + a. \end{aligned}$$

Multipliant par i^k, i^{km}, i^{km^2} et ajoutant, nous obtenons

$$\begin{aligned} -i^{k+3} - i^{(k+3)m} - i^{(k+3)m^2} = {} & c(i^{k+2} + i^{(k+2)m} + i^{(k+2)m^2})\\ & + b(i^{k+1} + i^{(k+1)m} + i^{(k+1)m^2}) + a(i^k + i^{km} + i^{km^2}), \end{aligned}$$

c'est-à-dire, en changeant les signes,

$$(2) \qquad -c_{k+3} = cc_{k+2} + bc_{k+1} + ac_k,$$

formule de récurrence qui, de proche en proche, nous donnera les c_k successivement.

Enfin,

$$b_k = i^{k(1+m+m^2)}\left(\frac{1}{i^k} + \frac{1}{i^{km}} + \frac{1}{i^{km^2}}\right) = (-a)^k(i^{-k} + i^{-km} + i^{-km^2});$$

et l'équation réductrice nous donne

$$\begin{aligned} 1 + ci^{-1} + bi^{-2} + ai^{-3} &= 0,\\ 1 + ci^{-m} + bi^{-2m} + ai^{-3m} &= 0,\\ 1 + ci^{-m^2} + bi^{-2m^2} + ai^{-3m^2} &= 0. \end{aligned}$$

Multipliant par i^{-k}, i^{-km}, i^{-km^2}, et ajoutant, il vient, en raison de la valeur de b_k écrite ci-dessus,

$$\frac{b_k}{(-a)^k} + c\frac{b_{k+1}}{(-a)^{k+1}} + b\frac{b_{k+2}}{(-a)^{k+2}} + a\frac{b_{k+3}}{(-a)^{k+3}} = 0,$$

ou

$$(3) \qquad b_{k+3} = bb_{k+2} - acb_{k+1} + a^2 b_k,$$

nouvelle formule de récurrence.

Par conséquent, si nous connaissons, en dehors de l'équation réductrice, les équations ayant i^2 d'une part, i^3 de l'autre, pour racines, nous en déduirons, par de simples formules linéaires, celles qui admettent i^4, i^5, ...

Or, les deux équations dont nous parlons sont l'équation aux carrés et l'équation aux cubes des racines de l'équation réductrice. Elles sont faciles à former par des procédés classiques.

Plus simplement peut-être encore, nous prendrons dans la Table les expressions de i^4, i^6 sous la forme

$$i^4 = \gamma i^2 + \beta i + \alpha,$$
$$i^6 = \gamma' i^2 + \beta' i + \alpha,$$

et l'élimination de i nous donnera une équation du troisième degré en i^2, qui est l'une de celles que nous cherchons.

De même, nous aurons la seconde en écrivant les valeurs de i^3, i^6, i^9, et en éliminant i et i^2 entre ces trois relations, ce qui donnera une équation en i^3.

Du reste, on arriverait directement à l'équation cherchée dont i^k est racine, en prenant dans la Table les expressions

$$i^k = C i^2 + B i + A,$$
$$i^{2k} = C' i^2 + B' i + A',$$
$$i^{3k} = C'' i^2 + B'' i + A'',$$

et en éliminant i^2 et i entre ces trois relations; en remplaçant i^k par x, on aurait une équation en x du troisième degré, qui ne serait autre que celle que l'on cherche.

Nous croyons devoir borner là nos observations particulières concernant le troisième degré.

NOTE I.

SUR LES MODULES COMPOSÉS.

Dans ce qui précède, l'étude des fonctions arithmétiques a été faite, en principe, en supposant le module premier; sauf dans quelques cas exceptionnellement simples, comme celui du premier degré.

Nous nous proposons ici, en les illustrant de quelques exemples, d'exposer certains principes, d'après lesquels on pourrait aborder en général le cas des modules composés, au moins en ce qui concerne les racines réelles des équations.

Le premier de ces principes est celui des abaques, dont on trouve déjà l'application dans notre ouvrage *Espaces arithmétiques hypermagiques,* et que nous pouvons rappeler rapidement ici, en ce qui concerne l'objet qui nous occupe. Si $m = pq$, p et q étant premiers entre eux, et si nous considérons l'équation $f(x) = 0$ par rapport au module m, on aura également $f(x) = 0$, modules p et q. En supposant que ces deux dernières équations aient été séparément résolues, la superposition des solutions donnera réciproquement la solution par rapport au module m. On comprend immédiatement que, de proche en proche, la résolution se ramènera ainsi au cas d'un module premier ou à celui d'un module de la forme a^α.

Pour éclaircir ceci par un exemple, dès le début, prenons l'équation incomplète

$$x^4 + dx^3 + a = 0 \qquad (\mathrm{mod}\ 15),$$

dont la famille peut être représentée par l'espace résolvant à deux dimensions (*fig.* 59).

Équation $x^4 + dx^3 + a \equiv 0 \pmod{15}$.

Fig. 59.

a \ d	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0					5, 10				3, 6 9, 12					1, 2, 4 7, 8, 11 13, 14
1	0, 5 9, 14	7, 8		6, 11			2, 12	13			4, 10		3	1	
2	0, 3 10, 13	14		7 8, 12			4, 9	11			5		1, 6	2	
3	0 12		4, 14	3		2, 5, 7 8, 10	6		13			1, 11	9		
4	0, 5 6, 11	13		9, 14			3	7, 8			1, 10		2, 12	4	
5	0 10				2 11, 14					1, 3, 4, 6 7, 8, 9 12, 13	5				
6	0 9		13	6		4, 5 10, 14	12		1, 11			2 7, 8	3		
7	0 3, 5	4		2, 12			9, 14	1			10, 13		6, 11	7, 8	
8	0, 7, 8 10, 12	11		3, 13			1, 6	14			2, 5		4, 9		
9	0 6		2 7, 8	9		1, 5 10, 11	3		4, 14			13	12		
10	0 5				1, 4, 7 8, 13					2, 3, 6 9, 11 12, 14	10				
11	0, 4 9, 10	2		1, 6			7 8, 12				5, 14		3, 13	11	
12	0 3		1 11	12		5 10, 13	9		2 7, 8			4, 14	6		
13	0, 2 5, 12	1		3			6, 11	4			7 8, 10		9, 14	13	
14	0, 1 6, 10			4, 9			3, 13	2			5, 11		7 8, 12	14	

Ce Tableau contient 15 cases sur chaque côté; divisons-le successivement en grandes cases, de côté 5 et de côté 3.

Dans toutes les cases de côté 5, mettons la solution de l'équation

$$x^4 + dx^3 + a \equiv 0 \qquad (\mathrm{mod}\, 5);$$

dans celles de côté 3, mettons la solution de cette même équation, module 3, et superposons les deux Tableaux de manière que les cases des deux abaques coïncident une à une.

Prenons une case quelconque; prenons aussi tous les chiffres inscrits dans cette case, d'un côté dans l'abaque de module 5, de l'autre dans l'abaque de module 3; faisons toutes les combinaisons possibles d'un chiffre quelconque dans l'un et l'autre abaque, et, au moyen de la Table de numération, déterminons les chiffres correspondant au module composé, et nous avons les chiffres à inscrire dans le plan de module 3.5.

Si dans l'un des abaques une case est blanche, elle le sera dans le Tableau de module composé, ce qui donne la raison du nombre énorme de cases blanches, et de l'accumulation des chiffres dans chaque case.

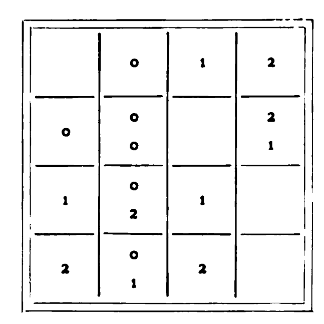
Pour voir comment les choses se passent, reproduisons d'abord la Table de numération module 15 = 3.5.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	0
1	2	3	4	0	1	2	3	4	0	1	2	3	4	0
1	2	0	1	2	0	1	2	0	1	2	0	1	2	0

Construisons ensuite (*fig.* 60) les plans donnant les solutions réelles pour chacun des modules (5, 3) :

Fig. 60.

	0	1	2	3	4
0	0 / 0				1 2 / 3 4
1	0 / 4	2	3	1	
2	0 / 3	4	1	2	
3	0 / 2	1	4	3	
4	0 / 1	3	2	4	



	0	1	2
0	0 / 0		2 / 1
1	0 / 2	1	
2	0 / 1	2	

Mettons chacun de ces Tableaux dans les grandes cases de l'abaque qui le concerne et nous avons les deux Tableaux de la figure 61 [1] :

---

[1] Pour simplifier, dans cette figure, on a laissé blanches les cases qui doivent devenir telles après la superposition.

Fig. 61.

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
		0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
0	0	0 0					0 0				1, 2 3, 4					1, 2 3, 4
1	1	0 4	2		1			2	3			0 4		3	1	
2	2	0 3	4		2			4	1			0 3		1	2	
3	3	0 2		4	3		0 2	1		3			1	4		
4	4	0 1	3		4			3	2			0 1		2	4	
5	0	0 0				1, 2 3, 4					1, 2 3, 4	0 0				
6	1	0 4		3	1		0 4	2		1			2	3		
7	2	0 3	4		2			4	1			0 3		1	2	
8	3	0 2	1		3			1	4			0 2		4		
9	4	0 1		2	4		0 1	3		4			3	2		
10	0	0 0				1, 2 3, 4					1, 2 3, 4	0 0				
11	1	0 4	2		1			2				0 4		3	1	
12	2	0 3		1	2		0 3	4		2			4	1		
13	3	0 2	1		3			1	4			0 2		4	3	
14	4	0 1			4			3	2			0 1		2	4	

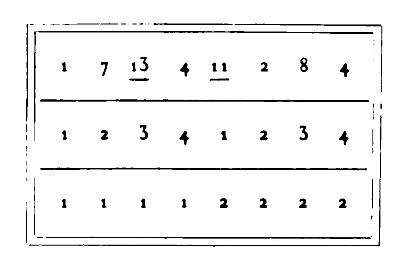
Fig. 61.

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
		0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
0	0	0 0					1 2				0 0					1 2
1	1	0 2	1		0 2			0 2	1			1		0 2	1	
2	2	0 1	2		0 1			0 1	2			2		0 1	2	
3	0	0 0		1 2	0 0		1 2	0 0		1 2			1 2	0 0		
4	1	0 2	1		0 2			0 2	1			1		0 2	1	
5	2	0 1				2					0 1	2				
6	0	0 0		1 2	0 0		1 2	0 0		1 2			1 2	0 0		
7	1	0 2	1		0 2			0 2	1			1		0 2	1	
8	2	0 1	2		0 1			0 1	2			2		0 1		
9	0	0 0		1 2	0 0		1 2	0 0		1 2			1 2	0 0		
10	1	0 2				1					0 2	1				
11	2	0 1	2		0 1			0 1				2		0 1	2	
12	0	0 0		1 2	0 0		1 2	0 0		1 2			1 2	0 0		
13	1	0 2	1		0 2			0 2	1			1		0 2	1	
14	2	0 1			0 1			0 1	2			2		0 1	2	

Prenons maintenant une case un peu chargée pour montrer le mécanisme dans toute sa complication.

Soit la case o $\underline{14}$; dans l'abaque de module 5, nous trouvons (1, 2, 3, 4); dans l'abaque de module 3, nous trouvons (1, 2).

Faisons toutes les associations possibles d'un des chiffres de l'abaque de module 5 avec un quelconque de ceux de l'abaque de module 3; nous avons le Tableau suivant, qui contient en outre le nombre correspondant de module 15 donné par la Table de numération; case o $\underline{14}$ du Tableau de la figure 59, nous trouvons effectivement ces huit chiffres et ceux-là seulement.



1	7	$\underline{13}$	4	$\underline{11}$	2	8	4
1	2	3	4	1	2	3	4
1	1	1	1	2	2	2	2

L'opération est si simple qu'il semble inutile de s'étendre davantage sur ce sujet.

Si nous faisons l'opération inverse, si nous prenons le Tableau de module composé et si nous écrivons chacun des chiffres inscrits dans le système de numération correspondant à chaque abaque, nous retrouvons les deux Tableaux ci-dessus.

Le lecteur peut constituer par ce procédé des espaces à un nombre quelconque de dimensions, et à un nombre quelconque de modules composants; puis observer à sa fantaisie tel fait graphique pouvant l'intéresser.

L'exemple ci-dessus peut servir de type pour les modules composés de la forme $a^1 b^1 c^1 \ldots$ dans lesquels chaque facteur n'entre qu'à la première puissance; s'il y a des facteurs de la forme a^α, la procédure est la même; la seule chose qui diffère consiste en ce que *pour les modules composés le chiffre* o *peut avoir, pour racines d'un certain indice, des nombres différents de* o.

Pour ne laisser aucune ombre dans l'esprit du lecteur, je vais résoudre l'équation $x^4 + bx + a = 0$, module $8 = 2^3$.

Formons le Tableau des puissances quatrièmes et des racines quatrièmes des chiffres de 8.

0	1	2	3	4	5	6	7	x
0	1	0	1	0	1	0	1	x^4
0, 2 4, 6	1, 3 5, 7							$\sqrt[4]{x}$

Un coup d'œil jeté sur ce Tableau montre que 0, pour le module 8, a pour racines quatrièmes quatre chiffres dont trois différents de 0, de sorte que, dans la ligne $b = 0$ du plan résolvant, la case dans laquelle $a = 0$ contiendra 0, 2, 4, 6, fait qui ne peut se produire quand le module m est un nombre de la forme a^1, et qui est spécial aux modules de forme a^α.

C'est là d'ailleurs la seule modification dans la construction des espaces, ainsi qu'on peut s'en convaincre dans le Tableau (*fig.* 62) résolvant l'équation $x^4 + bx + a = 0$, module 8.

Fig. 62.

	0	1	2	3	4	5	6	7
0	0, 2 4, 6							1, 3 5, 7
1	0, 2 4, 6						1, 3 5, 7	
2	0, 2 4, 6					1, 3 5, 7		
3	0, 2 4, 6				1, 3 5, 7			
4	0, 2 4, 6			1, 3 5, 7				
5	0, 2 4, 6		1, 3 5, 7					
6	0, 2 4, 6	1, 3 5, 7						
7	Tous							

Si nous avions à résoudre l'équation

$$x^2 + bx + a = 0,$$

l'opération préparatoire serait :

0	1	2	3	4	5	6	7	x
0	1	4	1	0	1	4	1	x^2
0 4	1, 3 5, 7			2 6				$\sqrt[2]{x}$

et le plan résolvant se construirait d'une façon analogue (*fig.* 63) :

Fig. 63.

	0	1	2	3	4	5	6	7
0	0, 4				2, 6			1, 3 5, 7
1	0, 4 2, 6						1, 3 5, 7	
2	0, 4				2, 6	1, 3 5, 7		
3	0, 4 2, 6				1, 3 5, 7			
4	0, 4			1, 3 5, 7	2, 6			
5	0, 4 2, 6		1, 3 5, 7					
6	0, 4	1, 3 5, 7			2, 6			
7	Tous							

Il me semble inutile de faire remarquer que si, dans un espace de module composé, on ne veut étudier qu'une faible portion de l'espace

de forme quelconque, il n'est pas nécessaire de construire l'espace tout entier, mais seulement de situer, dans l'espace à étudier, chacun des espaces résolvants des modules composants, et, par des permutations cycliques des lignes et des colonnes, remplir les cases de l'espace objet de l'étude.

Ce qui précède s'applique aux équations de tous les degrés indistinctement.

On peut appliquer notamment les mêmes principes à la construction des Tables de division. Soit, par exemple, $m = 12$. Nous pouvons construire les deux Tableaux d'abaques (*fig.* 64) qui, par leur superposition, et à l'aide de la Table de numération, donneraient la Table de division demandée.

Fig. 64.

d

D		0	1	2	3	4	5	6	7	8	9	10	11
		0	1	2	0	1	2	0	1	2	0	1	2
0	0	0 1, 2			0 1, 2			0 1, 2			0 1, 2		
1	1	0	1	2	0	1	2	0	1	2	0	1	2
2	2	0	2	1	0	2	1	0	2	1	0	2	1
3	0	0 1, 2			0 1, 2			0 1, 2			0 1, 2		
4	1	0	1	2	0	1	2	0	1	2	0	1	2
5	2	0	2	1	0	2	1	0	2	1	0	1	1
6	0	0 1, 2			0 1, 2			0 1, 2			0 1, 2		
7	1	0	1	2	0	1	2	0	1	2	0	1	2
8	2	0	2	1	0	2	1	0	2	1	0	2	1
9	0	0 1, 2			0 1, 2			0 1, 2			0 1, 2		
10	1	0	1	2	0	1	2	0	1	2	0	1	2
11	2	0	2	1	0	2	1	0	2	1	0	2	1

Fig. 64.

d	D												
		0	1	2	3	4	5	6	7	8	9	10	11
		0	1	2	3	0	1	2	3	0	1	2	3
0	0	0, 1 2, 3				0, 1 2, 3				0, 1 2, 3			
1	1	0	1	2	3	0	1	2	3	0	1	2	3
2	2	0 2		1 3		0 2		1 3		0 2		1 3	
3	3	0	3	2	1	0	3	2	1	0	3	2	1
4	0	0, 1 2, 3				0, 1 2, 3				0, 1 2, 3			
5	1	0	1	2	3	0	1	2	3	0	1	2	3
6	2	0 2		1 3		0 2		1 3		0 2		1 3	
7	3	0	3	2	1	0	3	2	1	0	3	2	1
8	0	0, 1 2, 3				0, 1 2, 3				0, 1 2, 3			
9	1	0	1	2	3	0	1	2	3	0	1	2	3
10	2	0 2		1 3		0 2		1 3		0 2		1 3	
11	3	0	3	2	1	0	3	2	1	0	3	2	1

La Table de division des modules composés joue d'ailleurs un rôle important, puisque, dans les Tables réduites de puissances de modules composés, telles que nous les avons décrites, on ne peut plus se servir des opérations sur les indices pour exécuter la division, les chiffres à diviser pouvant se trouver sur des lignes différentes de la Table des puissances.

Cette substitution d'opérations sur les indices ne peut s'exécuter d'une façon absolument générale que dans les cas où $\psi(m) = \varphi(\mathrm{M})$, autrement dit, où la Table ne contient qu'une seule ligne.

La division, pour les modules composés, a du reste une importance extrême pour l'étude des modules premiers, puisqu'on s'y trouve conduit à des opérations sur les indices, et qu'en ce cas le module des indices est nécessairement composé.

NOTE II.

SUR L'INDICATEUR.

L'indicateur $\varphi(m)$ d'un nombre m joue un rôle capital en Arithmétique. Dans nos *Espaces arithmétiques* (p. 79-81), nous en avons présenté la théorie, fondée sur la considération graphique fondamentale que voici : Soit, sur un espace à une dimension de module m, une marche régulière partant de l'origine, et de pas p; elle rencontrera les cases p, $2p$, ...; si cette marche rencontre toutes les cases avant d'atteindre de nouveau la case origine o, on dit qu'elle est parfaite, ou encore que p et m sont premiers entre eux, et alors l'indicateur $\varphi(m)$ est le nombre des marches parfaites possibles. Sinon la marche est imparfaite. Évidemment, la somme de l'indicateur et du nombre des marches imparfaites est m.

Cette considération, appliquée à $m = 1$, conduit très naturellement à $\varphi(1) = 1$, ou encore à ce résultat, un peu bizarre d'après les définitions ordinaires, que 1 est premier avec lui-même. Cela a été la cause de difficultés de langage qui n'ont échappé ni à Gauss, ni à Poinsot, ni à Lucas. La vision graphique, au contraire, donne à toute cette théorie une entière clarté.

Rappelons que, si m est premier,

$$\varphi(m) = m - 1;$$

que, si $m = pqr\ldots$, $p, q, r, \ldots$ étant premiers entre eux deux à deux,

$$\varphi(m) = \varphi(p)\,\varphi(q)\,\varphi(r)\ldots,$$

et qu'enfin, pour $m = a^\alpha b^\beta c^\gamma\ldots$, on a

$$\varphi(m) = (a-1)(b-1)(c-1)\ldots a^{\alpha-1} b^{\beta-1} c^{\gamma-1}\ldots.$$

Un autre élément, non moins essentiel, et que l'on rencontre à chaque instant, est l'*indicateur réduit*. Si $m = pqr\ldots$, $p, q, r, \ldots$ étant premiers entre eux deux à deux, le plus petit comultiple des indica-

teurs $\varphi(p)$, $\varphi(q)$, $\varphi(r)$, ..., de p, q, r, ... est ce qu'on appelle l'*indicateur réduit* de m. On le désigne par $\psi(m)$.

Il résulte de ceci que, pour calculer l'indicateur réduit de

$$m = a^\alpha b^\beta c^\gamma \ldots,$$

il y a lieu de calculer les indicateurs de a^α, b^β, c^γ, ... qui sont

$$a^{\alpha-1}(a-1), \quad \ldots.$$

Mais, s'il arrive que a soit égal à 2 et que α soit supérieur à 2, on doit écrire

$$\psi(2^\alpha) = \frac{1}{2}\varphi(2^\alpha),$$

pour le calcul du plus petit comultiple. La raison de cette apparente exception est que, pour tout nombre impair k (c'est-à-dire pour un nombre premier avec 2), on a toujours l'équation congruente par rapport à $m = 2^\alpha$

$$k^{2^{\alpha-2}} = 1.$$

La vraie définition générale de l'indicateur réduit d'un nombre m quelconque est en réalité la suivante, dont on a constamment occasion de constater l'utilité :

L'indicateur réduit d'un nombre m est le plus petit nombre p tel qu'on ait toujours, *quel que soit le chiffre a premier avec m*,

$$a^p - 1 = 0,$$

en congruant suivant m.

Ainsi posée, elle ne comporte aucune exception.

Quant à l'anomalie que présente en apparence le facteur premier 2, elle provient, au fond, de ce que tous les nombres par rapport à un nombre premier m quelconque, autre que 2, peuvent s'écrire sous l'une des formes

$$\text{mult.}\, m, \quad \text{mult.}\, m \pm 1, \quad \text{mult.}\, m \pm 2, \quad \ldots$$

tandis que, pour $m = 2$, si un nombre n'est pas multiple de 2, il a la forme unique mult. $2 + 1$, les deux formes mult. 2 ± 1 se confondant en une seule.

D'après le procédé de calcul qui précède, on voit immédiatement que, suivant la remarque très juste de Lucas, l'indicateur réduit $\psi(m)$ se confond avec l'indicateur $\varphi(m)$:

1° Pour $m = 2$;

2° Pour $m = 4$;
3° Pour $m = a^{\alpha}$, a étant premier impair;
4° Pour $m = 2a^{\alpha}$.

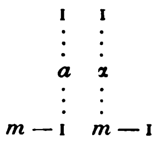
Dans tous les autres cas, $\psi(m)$ est un diviseur de $\varphi(m)$.

NOTE III.

SUR LE THÉORÈME DE WILSON.

Ce théorème est d'une extrême importance dans la théorie des nombres, puisqu'il donne un *criterium* certain caractérisant un nombre premier, au point de vue théorique; malheureusement, l'application pratique devient irréalisable pour des nombres un peu grands.

Les Tables de division, pour un module m premier, fournissent de ce théorème de Wilson une démonstration extrêmement simple. En accolant à la colonne des diviseurs, extérieure au cadre, la première colonne de la Table, qui correspond au dividende 1, nous avons un Tableau :



dans lequel $a\alpha = 1$; d'ailleurs a et α ne peuvent être égaux que pour la première et la dernière ligne, car $x^2 - 1 = 0$, le module étant premier, ne peut donner que $x = 1$ ou $x = -1 = m - 1$.

Donc, en supprimant ces deux lignes extrêmes et conservant la moitié seulement des couples $a\alpha$ de façon que, dans l'ensemble, il n'y ait que deux chiffres égaux, nous aurons par multiplication

$$2.3\ldots(m-2) = 1,$$

et, introduisant le facteur $1(m-1) = -1$,

$$(m-1)! = -1.$$

NOTE IV.

AU SUJET DES TABLES DE PUISSANCES D'IMAGINAIRES.

Quand une Table complète de puissances d'imaginaires a été dressée

$$i, \quad i^2, \quad \ldots, \quad i^{m^n-1} = 1,$$

pour un module m et un degré n, en partant d'une équation réductrice convenable, tous les i^k sont exprimés par des polynomes en i, de degré $n - 1$ au plus.

Si l'on donne un terme i^k particulier, il peut y avoir intérêt à savoir de quelle équation ce terme est racine. Nous avons donné (Chap. VI) une solution de cette question, fondée sur le calcul, assez pénible, des fonctions symétriques de

$$i^k, \quad i^{km}, \quad i^{km^2}, \quad \ldots, \quad i^{km^{n-1}},$$

qui sont les racines de l'équation cherchée.

Or, généralisant ce que nous avons exposé à la fin du Chapitre IX pour le cas du troisième degré, nous trouvons une méthode beaucoup plus simple.

Cherchons dans la Table les termes i^{2k}, i^{3k}, $\ldots$, i^{nk}; nous aurons

$$\begin{aligned} i^k &= h_1\, i^{n-1} + \ldots + b_1\, i + a_1, \\ i^{2k} &= h_2\, i^{n-1} + \ldots + b_2\, i + a_2, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ i^{nk} &= h_n\, i^{n-1} + \ldots + b_n\, i + a_n. \end{aligned}$$

Si, entre ces n équations linéaires, nous éliminons les $n - 1$ lettres i, i^2, $\ldots$, i^{n-1}, il nous restera une équation linéaire en i^k, $\ldots$, i^{nk},

$$(1) \qquad A_n\, i^{nk} + A_{n-1}\, i^{(n-1)k} + \ldots + A_2\, i^{2k} + A_1\, i^k + A_0 = 0,$$

dont le premier membre peut s'écrire immédiatement sous forme de déterminant.

Cette identité (1) nous montre que i^k est racine de l'équation

$$A_n x^n + A_{n-1} x^{n-1} + \ldots + A_2 x^3 + A_1 x + A_0 = 0,$$

qui est par conséquent l'équation demandée.

NOTE V.

La démonstration (p. 40, n° 20) de l'importante proposition, qu'*il y a toujours des chiffres ayant pour gaussien un diviseur quelconque de* $m - 1$, semble ne pas être irréprochable; cela tient à la forme trop brève peut-être sous laquelle nous l'avons présentée, en nous inspirant de Lebesgue (*Introduction à la théorie des nombres*, p. 94).

Comme il s'agit d'un théorème classique, dont diverses démonstrations ont été apportées par plusieurs auteurs, il ne nous semble pas nécessaire de revenir plus longuement sur la question. Mais nous avons tenu à mettre le lecteur en garde, et à lui permettre de faire la rectification nécessaire, s'il le désire.

L'observation dont il s'agit nous a été communiquée par M. Gaston Tarry, auquel nous avions donné connaissance des épreuves, et que nous remercions sincèrement. Mais, malheureusement, elle ne nous parvient qu'après l'impression presque complète de notre livre.

FIN.

TABLE DES MATIÈRES.

CHAPITRE I.

MULTIPLICATION ET DIVISION DES ENTIERS.

CHAPITRE II.

PUISSANCES ET RACINES DES ENTIERS.

CHAPITRE III.

FONCTIONS RÉDUCTIBLES ET IRRÉDUCTIBLES.

CHAPITRE IV.

RACINES DE L'UNITÉ. IMAGINAIRES DE GALOIS.

CHAPITRE V.

RECHERCHE DES RACINES RÉELLES.

CHAPITRE VI.

RECHERCHE DES RACINES IMAGINAIRES.

CHAPITRE VII.

VARIATIONS DES FONCTIONS ARITHMÉTIQUES.

CHAPITRE VIII.

ÉTUDE DU PREMIER ET DU DEUXIÈME DEGRÉS.

CHAPITRE IX.

ETUDE DU TROISIÈME DEGRÉ.

NOTES.

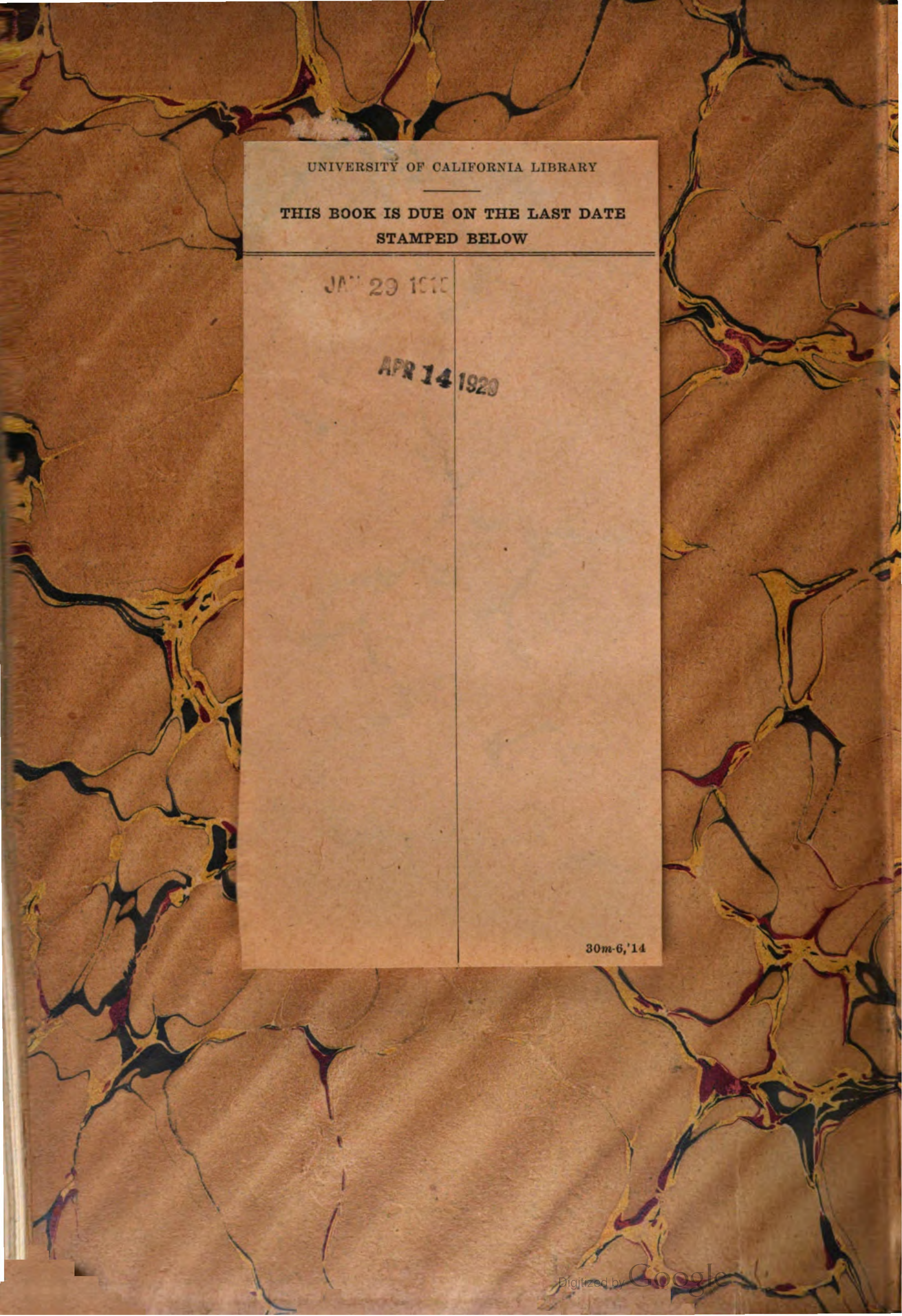


36964. Paris. — Imp. GAUTHIER-VILLARS, 55, quai des Grands-Augustins.

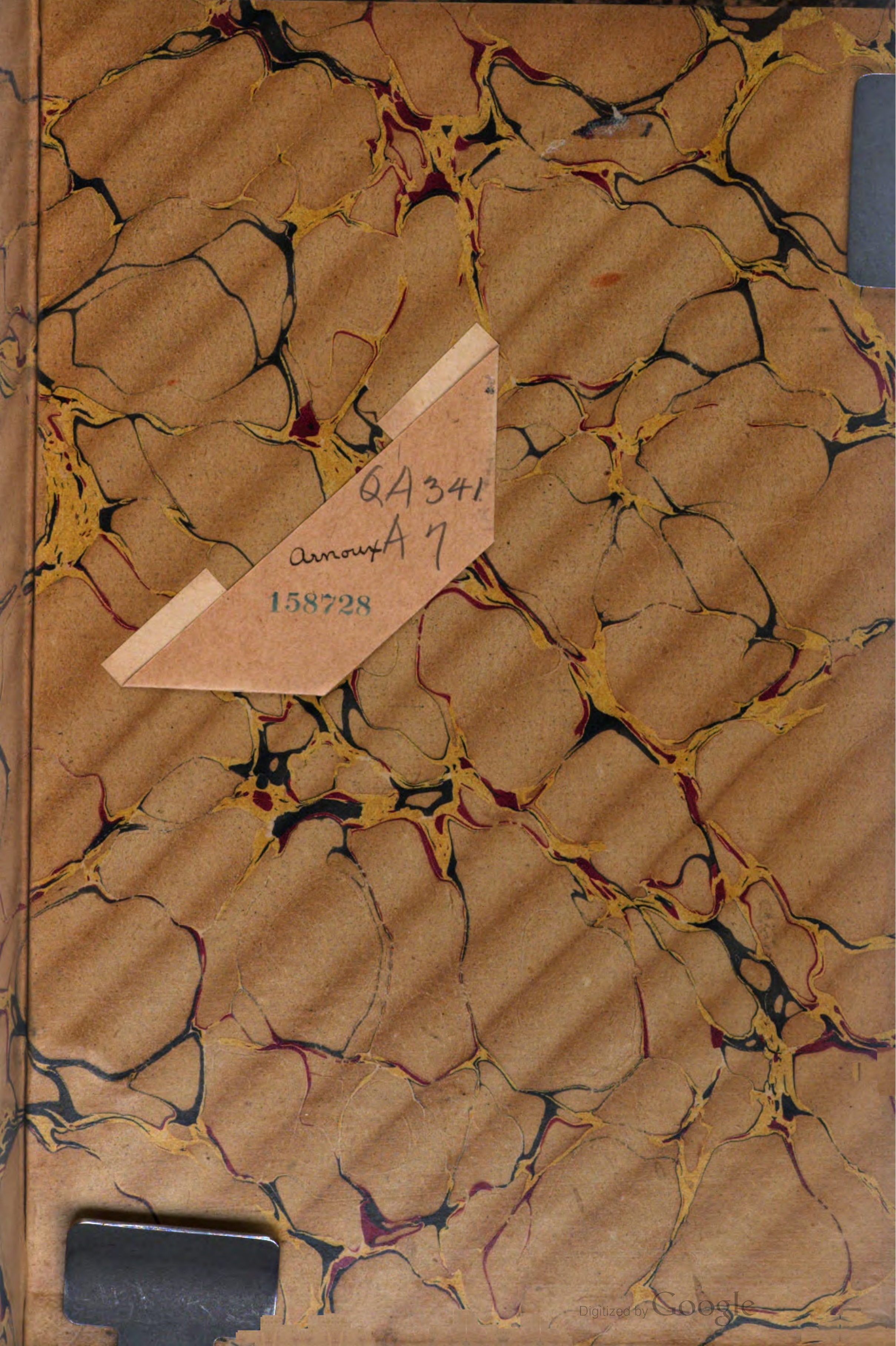
36964 PARIS. — IMPRIMERIE GAUTHIER-VILLARS,
Quai des Grands-Augustins, 55.




LABORA ET NOLI
CONTRISTARI



UNIVERSITY OF CALIFORNIA LIBRARY
THIS BOOK IS DUE ON THE LAST DATE
STAMPED BELOW
APR 14 1929
30m-6,'14


QA341
Arnoux A7
158728
Digitized by Google

